Cisco IOS Voice Commands: A

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the Cisco IOS Master Commands List online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

aal2-profile custom

To specify custom numbers and user-to-user information (UUI) code points for ATM adaptation layer 2 (AAL2) profiles and codecs, use the **aal2-profile custom** command in global configuration mode. To disable the configuration, use the **no** form of this command.

aal2-profile custom *number number number* {**clear-channel | g711alaw | g711ulaw | g726r32 | g729br8 | g720r8 | llcc**} *packet-length minimum-UUI-codepoint maximum-UUI-codepoint*

no aal2-profile custom *number*

Syntax Description

number	AAL profile number. For more information, use the question mark (?) online help function.
clear-channel | g711alaw | g711ulaw | g726r32 | g729br8 | g720r8 | llcc	Specifies the types of codec as follows: • Clear Channel • G.711 a-law • G.711-mu-law • G.726r32 • G.729 ANNEX-B 8000 bits per second • G.729 8000 bps • Lossless Compression
packet-length	Packet length in octets. The range is from 5 to 64.
minimum-UUI-codepoint	Minimim UUI code point. The range is from 0 to 15.
maximum-UUI-codepoint	Maximum UUI code point. The range is from 0 to 15.

Command Default

One of the predefined International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) profiles can be used.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

AAL2 custom profiles are used to define additional profiles that are not present in the ITU-T specifications.

After defining a custom profile, apply that profile under a Voice over ATM (VoATM) dial peer for it to take affect using the **codec aal2-profile** command. The **codec aal2-profile** command can be used only if the session protocol is "aal2-trunk".

Examples

The following example shows how to specify custom numbers and UUI cod epoints for AAL2 profiles and codecs:

```
Router# configure terminal
Router(config)# aal2-profile custom  2 1 1 g711ulaw 6 3 3
```

aaa nas port voip

To send out the standard NAS-port attribute (RADIUS IETF Attribute 5) on voice interfaces, use the **aaa nas port voip** command in global configuration mode. To disable the command, use the **no** form of the command.

aaa nas port voip

no aaa nas port voip

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5300.

Usage Guidelines This command brings back the original behavior of the Authentication, Authorization, and Accounting (AAA). NAS-Port on VoIP interfaces. By default this feature is disabled.

Examples The following example shows how to return to the original behavior of the AAA NAS-Port:

```
aaa nas port voip
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information.

aaa username

To determine the information with which to populate the username attribute for Authentication, Authorization, and Accounting (AAA). billing records, use the **aaa username** command in SIP UA configuration mode. To achieve default capabilities, use the **no** form of this command.

aaa username {**calling-number** | **proxy-auth**}

no aaa username

Syntax Description

calling-number	Uses the FROM: header in the SIP INVITE (default value). This keyword is used in most implementations.
proxy-auth	Parses the Proxy-Authorization header. Decodes the Microsoft Passport user ID (PUID) and password, and then populates the PUID into the username attribute and a "." into the password attribute. The username attribute is used for billing, and the "." is used for the password, because the user has already been authenticated before this point.

Command Default **calling-number**

Command Modes SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and the Cisco AS5400.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(11)T	This command was integrated Cisco IOS Release 12.2(11)T and was implemented on the Cisco AS5850. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.

Usage Guidelines Parsing the Proxy-Authorization header, decoding the PUID and password, and populating the username attribute with the PUID must be enabled through this command. If this command is not issued, the Proxy-Authorization header is ignored.

The keyword **proxy-auth** is a nonstandard implementation, and Session Initiation Protocol (SIP) gateways do not normally receive or process the Proxy-Authorization header.

Examples

The following example enables the processing of the SIP username from the Proxy-Authorization header:

```
Router(config)# sip-ua
Router(config-sip-ua)# aaa username proxy-auth
```

Related Commands

Command	Description
show call active voice	Displays sactive call information for voice calls or fax transmissions in progress.
show call history voice	Displays the voice call history table.

access-list (voice source-group)

To assign an access list to a voice source group, use the **access-list** command in voice source-group configuration mode. To delete the access list, use the **no** form of this command.

access-list *access-list-number*

no access-list *access-list-number*

Syntax Description

access-list-number	Number of an access list. The range is from 1 to 99.

Command Default

No default behavior or values

Command Modes

Voice source-group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced in voice source-group configuration mode.

Usage Guidelines

An access list defines a range of IP addresses for incoming calls that require additional scrutiny. Two related commands are used for voice source groups:

- Use the **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] command in global configuration mode to define the contents of the access list.
- Use the **access-list** *access-list-number* command in voice source-group configuration mode to assign the defined access list to the voice source group.

The terminating gateway uses the source IP group to identify the source of the incoming VoIP call before selecting an inbound dial peer. If the source is found in the access list, then the call is accepted or rejected, depending on how the access list is defined.

The terminating gateway uses the access list to implement call blocking. If the call is rejected, the terminating gateway returns a disconnect cause to the source. Use the **disconnect-cause** command to specify a disconnect cause to use for rejected calls.

Use the **show access-lists** privileged EXEC command to display the contents of all access lists.

Use the **show ip access-lis**t privileged EXEC command to display the contents of one access list.

Examples

The following example assigns access list 1 to voice source-group alpha. Access list 1 was defined previously using another command. An incoming source IP group call is checked against the conditions defined for access list 1 and is processed based on the permit or deny conditions of the access list.

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# access-list 1
```

Related Commands

Command	Description
carrier-id (dial peer)	Specifies the carrier as the source of incoming VoIP calls (for carrier ID routing).
disconnect-cause	Specifies a cause for blocked calls.
h323zone-id (voice source group)	Associates a zone for an incoming H.323 call.
show access-lists	Displays the contents of all access lists.
show ip access-list	Displays the contents of one access list.
translation-profile (source group)	Associates a translation profile with incoming source IP group calls.
trunk-group-label (voice source group)	Specifies the trunk group as the source of incoming VoIP calls (for trunk group label routing).
voice source-group	Initiates the source IP group profile definition.

access-policy

To require that a neighbor be explicitly configured in order for requests to be accepted, use the **access-policy** command in Annex G configuration mode. To reset the configuration to accept all requests, use the **no** form of this command.

access-policy [**neighbors-only**]

no access-policy

Syntax Description

neighbors-only	(Optional) Requires that a neighbor be configured.

Command Default

Border elements accept any and all requests if service relationships are not configured.

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Border elements accept any and all requests if service relationships are not configured. The **access-policy** command eliminates arbitrary requests from unknown border elements, and is a required prerequisite for configuring service relationships.

Examples

The following example shows how to enable the service relationship between border elements:

```
Router(config-annexg)# access-policy neighbors-only
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
domain-name	Sets the domain name reported in service relationships.

accounting (gatekeeper)

To enable and define the gatekeeper-specific accounting method, use the **accounting** command in gatekeeper configuration mode. To disable gatekeeper-specific accounting, use the **no** form of this command.

accounting {**username h323id** | **vsa**}

no accounting

Syntax Description

username h323id	Enables H323ID in the user name field of accounting record.
vsa	Enables the vendor specific attribute accounting format.

Command Default Accounting is disabled.

Command Modes Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **vsa** keyword was added.
12.2(2)T	The **vsa** keyword was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(9)T	This **username h323id** keyword was added.

Usage Guidelines To collect basic start-stop connection accounting data, the gatekeeper must be configured to support gatekeeper-specific H.323 accounting functionality. The **accounting** command enables you to send accounting data to the RADIUS server via IETF RADIUS or VSA attriibutes.

Specify a RADIUS server before using the **accounting** command.

There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.

Examples The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

The following example configures H.323 accounting using IETF RADIUS attributes:

```
Router(config-gk)# accounting username h323id
```

The following example configures H.323 accounting using VSA RADIUS attributes:

```
Router(config-gk)# accounting vsa
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gatekeeper	Enters gatekeeper configuration mode.

accounting method

To set an accounting method at login for calls that come into a dial peer, use the **accounting method** command in voice class AAA configuration mode. To disable the accounting method set at login, use the **no** form of this command.

accounting method *MethListName* [**out-bound**]

no accounting method *MethListName* [**out-bound**]

Syntax Description

MethListName	Defines an accounting method list name.
out-bound	(Optional) Defines the outbound leg.

Command Default

When this command is not used to specify an accounting method, the system uses the **aaa accounting connection h323** command as the default. If the method list name is not specified, the outbound call leg uses the same method list name as the inbound call leg

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

This command sets the accounting method for dial peers in voice class AAA configuration mode. To initially define a method list, refer to the *Cisco IOS Security Configuration Guide,* Release 12.2.

If the outbound option is specified, the outbound call leg on the dial peer uses the method list name specified in the command. If the method list name is not specified, by default, the outbound call leg uses the same method list name as the inbound call leg.

Examples

The following example sets the dp-out method for the outbound leg:

```
voice class aaa 1
 accounting method dp-out out-bound
```

Related Commands

Command	Description
aaa accounting connection h323	Defines the accounting method list H.323 with RADIUS, using **stop-only** or **start-stop** accounting options.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

accounting suppress

To disable accounting that is automatically generated by a service provider module for a specific dial peer, use the **accounting suppress** command in voice class AAA configuration mode. To allow accounting to be automatically generated, use the **no** form of this command.

accounting suppress [**in-bound** | **out-bound**]

no accounting suppress [**in-bound** | **out-bound**]

Syntax Description

in-bound	(Optional) Defines the call leg for incoming calls.
out-bound	(Optional) Defines the call leg for outbound calls.

Command Default

Accounting is automatically generated by the service provider module.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

If a call leg option is not specified by the command, accounting is disabled for both inbound and outbound calls. For accounting to be automatically generated in the service provider module, you must first configure **gw-accounting aaa** command in global configuration mode before configuring dial-peer-based accounting in voice class AAA configuration mode.

Examples

In the example below, accounting is suppressed for the incoming call leg.

```
voice class aaa 1
 accounting suppress in-bound
```

Related Commands

Command	Description
gw-accounting aaa	Enables VoIP gateway accounting.
suppress	Turns off accounting for a call leg on a POTS or VoIP dial peer. This command is used in gw-accounting aaa configuration mode.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

accounting template

To allow each dial peer to choose and send a customized accounting template to the RADIUS server, use the **accounting template** command in voice class AAA configuration mode. To disable the dial peer from choosing and sending a customized accounting template, use the **no** form of this command.

accounting template *acctTempName* [**out-bound**]

no accounting template *acctTempName* [**out-bound**]

Syntax Description

acctTempName	Defines an accounting template name.
out-bound	(Optional) Defines the outbound leg.

Command Default

The dial peer does not choose and send a customized accounting template to the RADIUS server.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

By default, non-RFC-mandatory vendor-specific attributes (VSAs) are not included in accounting records if you do not configure the accounting template. The accounting template enables you to manage accounting records at a per-VSA level. When an accounting template is used for customizing the accounting record, the VSA name release source has to be included in the template file so that it is included in the accounting record and sent to the RADIUS server.

This command overrides the **acct-template** command in gateway accounting AAA configuration mode when a customized accounting template is used.

If you use a Tool Command Language (Tcl) script, the Tcl verb **aaa accounting start** [**-t acctTempName**] takes precedence over the **accounting template** command in voice class AAA configuration mode.

Examples

The following example sets the template temp-dp for the outbound leg

```
voice class aaa 1
 accounting template temp-dp out-bound
```

Related Commands

Command	Description
acct-template	Sends a selected group of voice accounting VSAs.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

acc-qos

To define the acceptable quality of service (QoS) for any inbound and outbound call on a VoIP dial peer, use the **acc-qos** command in dial peer configuration mode. To restore the default QoS setting, use the **no** form of this command.

acc-qos {**best-effort** | **controlled-load** | **guaranteed-delay**} [**audio** | **video**]

no acc-qos

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.
controlled-load	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.
audio	(Optional) Configures acceptable QoS for audio traffic.
video	(Optional) Configures acceptable QoS for video traffic.

Command Default **best-effort**

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.1(5)T	The description of the command was modified.
12.3(4)T	The **audio** and **video** keywords were added.

Usage Guidelines This command is applicable only to VoIP dial peers.

When VoIP dial peers are used, the Cisco IOS software uses RSVP to reserve a certain amount of bandwidth so that the selected QoS can be provided by the network. Call setup is aborted if the RSVP resource reservation does not satisfy the acceptable QoS for both peers.

To select the most appropriate value for this command, you need to be familiar with the amount of traffic this connection supports and what kind of impact you are willing to have on it. The Cisco IOS software generates a trap message when the bandwidth required to provide the selected quality of service is not available.

If **audio** or **video** is not configured, the bearer capability information element (IE) is not checked against max values during SETUP.

You must use the **ip rsvp bandwidth** command to enable RSVP on an IP interface before you can specify RSVP QoS.

In order to use this command, you have to have the **req-qos** statement present.

Examples

The following example selects **guaranteed-delay** as the acceptable QoS for inbound and outbound audio calls on VoIP dial peer 10:

```
dial-peer voice 10 voip
 acc-qos guaranteed-delay
```

The following example selects **controlled-load** as the acceptable QoS for audio and video:

```
dial-peer voice 100 voip
 acc-qos controlled-load audio
 acc-qos controlled-load video
```

Related Commands

Command	Description
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.

acct-template

To select a group of voice attributes to collect in accounting records, use the **acct-template** command in gateway accounting AAA or gateway accounting file configuration mode. To disable collection of a group of voice attributes, use the **no** form of this command.

acct-template {*template-name* | **callhistory-detail**}

no acct-template {*template-name* | **callhistory-detail**}

Syntax Description

template-name	Name of the custom accounting template.
callhistory-detail	Collects all voice vendor-specific attributes (VSAs) for accounting.

Command Default

No voice attributes are collected.

Command Modes

Gateway accounting AAA configuration (config-gw-accounting-aaa)
Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)XY	This command was added to gateway accounting file configuration mode.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to collect only the voice attributes that are defined in an accounting template. The accounting template is a text file that you create by selecting specific attributes that are applicable to your billing needs. Use the **call accounting-template voice** command to define your accounting template before using the **acct-template** command.

The **show call accounting-template voice master** command displays all the voice attributes that can be filtered by accounting templates.

Use the **callhistory-detail** keyword to send all voice VSAs to the accounting server. For a description of supported voice VSAs, see the "VSAs Supported by Cisco Voice Products" section in the *RADIUS VSA Voice Implementation Guide*.

When you send only those VSAs defined in your accounting template, the default call-history records that are created by the service provider are automatically suppressed.

Examples

The example below uses the **acct-template** command to specify temp-global, a custom template.

```
gw-accounting aaa
 acct-template temp-global
```

Related Commands

Command	Description
call accounting-template voice	Defines a customized accounting template.
gw-accounting	Enables the method of collecting accounting data.
show call accounting-template voice	Displays attributes defined in accounting templates.

activation-key

To define an activation key that can be dialed by phone users to activate Call Back on Busy on an analog phone, use the **activation-key** command in STC application feature callback configuration mode. To return the code to its default, use the **no** form of this command.

activation-key *string*

no activation-key

Syntax Description

string	Character string that can be dialed on a telephone keypad (0-9, *, #). Length of string is one to five characters. Default: #1.

Command Default Callback activation key is #1.

Command Modes STC application feature callback configuration (config-stcapp-callback)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines This command changes the value of the callback activation key for Call Back on Busy from the default (#1) to the specified value.

To display information about the Call Back configuration, use the **show stcapp feature codes** command.

Examples The following example shows how to change the value of the callback activation key sequence from the default (#1) to a new value (*22).

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)# activation-key *22
Router(config-stcapp-callback)#
```

The following partial output from the **show stcapp feature codes** command displays values for the call back feature:

```
Router# show stcapp feature codes

.
.
.

  stcapp feature callback
    key *1
    timeout 30
```

Related Commands

Command	Description
ringing-timeout	Defines the timeout period for Callback on Busy.
show stcapp feature codes	Displays all feature codes for FACs, FSDs, and call back.

address-family (tgrep)

To set the global address family to be used on all dial peers, use the **address-family** command in TGREP configuration mode. To change back to the default address family, use the **no** form of this command.

address family {**e164** | **decimal** | **penta-decimal**}

no address family {**e164** | **decimal** | **penta-decimal**}

Syntax Description

e164	E.164 address family.
decimal	Digital address family.
penta-decimal	Pentadecimal address family.

Command Default E.164 address family

Command Modes TGREP configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines The E. 164 address family is used if the telephony network is a public telephony network. Decimal and pentadecimal options can be used to advertise private dial plans. For example, if a company wants to use TRIP in within its enterprise telephony network using five-digit extensions, then the gateway would advertise the beginning digits of the private numbers as a decimal address family. These calls cannot be sent out of the company's private telephony network because they are not E.164-compliant.

The pentadecimal family allows numbers 0 through 9 and alphabetic characters A through E and can be used in countries where letters are also carried in the called number.

Examples The following example shows that the address family for itad 1234 is set for E.164 addresses:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# address family e164
```

Related Commands

Command	Description
tgrep local-itad	Enters TGREP configuration mode and defines an ITAD.

address-hiding

To hide signaling and media peer addresses from endpoints other than the gateway use the **address-hidding** command in voice-service configuration mode. To allow the peer address known to all endpoints, use the **no** form of this command.

address-hiding

no address-hiding

Syntax Description There are no keywords or aruguments.

Command Default Signaling and media addresses are visable to all endpoints.

Command Modes Voice-service configuration mode

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines All SIP methods/messages should terminate at IP-to-IP gateway and re-originate with IP-to-IP gateway address, address hiding makes the peer address known only to the IP-to-IP gateway. Hiding address in flow-through mode is required for SIP-to-SIP in an IP-to-IP gateway network.

Note Distinctive ringing headers include ringing information and server address where the ring tone can be optained. These headers will be forwarded as is to the peer side even if address hiding is enabled.

Examples The following example show address-hiding being configured for all VoIP calls:

```
Router(config)# voice service voip
Router(config-voi-serv) address-hiding
```

Related Commands

Command	Description
voice service	Enters voice-service configuration mode.

advertise (annex g)

To control the types of descriptors that the border element (BE) advertises to its neighbors, use the **advertise** command in Annex G configuration mode. To reset this command to the default value, use the **no** form of this command.

advertise [**static** | **dynamic** | **all**]

no advertise

Syntax Description

static	(Optional) Only the descriptors provisioned on this BE is advertised. This is the default.
dynamic	(Optional) Only dynamically learned descriptors is advertised.
all	(Optional) Both static and dynamic descriptors is advertised.

Defaults

Static

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example configures a BE that advertises both static and dynamic descriptors to its neighbors:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# advertise all
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
show call history	Displays the routes stored in cache for the BE.
show call-router status	Displays the Annex G BE status.

advertise (tgrep)

To turn on reporting for a specified address family, use the **advertise** command in TGREP configuration mode. To turn off reporting for a specified address family, use the **no** form of this command.

advertise {**e164 | decimal | penta-decimal** }[**csr**][**ac**][**tc**][**trunk-group | carrier**]

advertise {**trunk-group | carrier**}[**csr**][**ac**][**tc**]

no advertise {**e164 | decimal | penta-decimal | trunk-group | carrier**}

Syntax Description

e164	E.164 address family.
decimal	Decimal address family
penta-decimal	Penta-decimal address family
trunk-group	Trunk group address family
carrier	Carrier code address family
csr	Call success rate
ac	Available circuits
tc	Total circuits

Command Default No attributes for address families are advertised.

Command Modes TGREP configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines If you specify **e164**, **decimal** or **penta-decimal** for the address family, you can stipulate whether the related **carrier** or **trunk-group** parameters are advertised. If you stipulate **carrier** or **trunk-group** for the address family, you can stipulate that the related address family prefix is advertised. If you stipulate **carrier** or **trunk-group** for the address family, you cannot stipulate **carrier** or **trunk-group** attributes for advertising.

When the **no** version of this command is used, it turns off the advertisement of that particular address family altogether.

Examples The following example shows that the E.164 address family with call success rate, available circuits, total circuits, and trunk group attributes is being advertised for ITAD 1234:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# advertise e164 csr ac tc trunk-group
```

Related Commands

Command	Description
tgrep local-itad	Enters TGREP configuration mode and defines an ITAD.

alarm-trigger

To configure a T1 or E1 controller to send an alarm to the public switched telephone network (PSTN) or switch if specified T1 or E1 DS0 groups are out of service, use the **alarm-trigger** command in controller configuration mode. To configure a T1 or E1 controller not to send an alarm, use the **no** form of this command.

alarm-trigger blue *ds0-group-list*

no alarm-trigger

Syntax Description

blue	Specifies the alarm type to be sent is "blue," also known as an Alarm Indication Signal (AIS).
ds0-group-list	Specifies the DS0 group or groups to be monitored for permanent trunk connection status or busyout status.

Command Default

No alarm is sent

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.

Usage Guidelines

Any monitored time slot can be used for either permanent trunk connections or switched connections. Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) can be combined on a T1 or E1 controller and monitored for alarm conditioning.

An alarm is sent only if all of the time slots configured for alarm conditioning on a T1 or E1 controller are out of service. If one monitored time slot remains in service or returns to service, no alarm is sent.

Examples

The following example configures T1 0 to send a blue (AIS) alarm if DS0 groups 0 and 1 are out of service:

```
controller t1 0
 alarm-trigger blue 0,1
 exit
```

Related Commands

Command	Description
busyout monitor	Configures a voice port to monitor an interface for events that would trigger a voice-port busyout.
connection trunk	Creates a permanent trunk connection (private line or tie-line) between a voice port and a PBX.
voice class permanent	Creates a voice class for a Cisco or FRF-11 permanent trunk.

alias static

To create a static entry in the local alias table, use the **alias static** command in gatekeeper configuration mode. To remove a static entry, use the **no** form of this command.

alias static *ip-signaling-addr* [*port*] **gkid** *gatekeeper-name* [**ras** *ip-ras-addr port*] [**terminal | mcu | gateway** {**h320 | h323-proxy | voip**}] [**e164** *e164-address*] [**h323id** *h323-id*]

no alias static *ip-signaling-addr* [*port*] **gkid** *gatekeeper-name* [**ras** *ip-ras-addr port*] [**terminal | mcu | gateway** {**h320 | h323-proxy | voip**}] [**e164** *e164-address*] [**h323id** *h323-id*]

Syntax Description

ip-signaling-addr	IP address of the H.323 node, used as the address to signal when establishing a call.
port	(Optional) Port number other than the endpoint Call Signaling well-known port number (1720).
gkid *gatekeeper-name*	Name of the local gatekeeper of whose zone this node is a member.
ras *ip-ras-addr*	(Optional) Node remote access server (RAS) signaling address. If omitted, the *ip-signaling-addr* parameter is used in conjunction with the RAS well-known port.
port	(Optional) Port number other than the RAS well-known port number (1719).
terminal	(Optional) Indicates that the alias refers to a terminal.
mcu	(Optional) Indicates that the alias refers to a multiple control unit (MCU).
gateway	(Optional) Indicates that the alias refers to a gateway.
h320	(Optional) Indicates that the alias refers to an H.320 node.
h323-proxy	(Optional) Indicates that the alias refers to an H.323 proxy.
voip	(Optional) Indicates that the alias refers to VoIP.
e164 *e164-address*	(Optional) Specifies the node E.164 address. This keyword and argument can be used more than once to specify as many E.164 addresses as needed. Note that there is a maximum number of 128 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple **alias static** commands with the same call signaling address and different aliases.
h323id *h323-id*	(Optional) Specifies the node H.323 alias. This keyword and argument can be used more than once to specify as many H.323 identification (ID) aliases as needed. Note that there is a maximum number of 256 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple **alias static** commands with the same call signaling address and different aliases.

Command Default No static aliases exist.

Command Modes Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

The local alias table can be used to load static entries by performing as many of the commands as necessary. Aliases for the same IP address can be added in different commands, if required.

Typically, static aliases are needed to access endpoints that do not belong to a zone (that is, they are not registered with any gatekeeper) or whose gatekeeper is inaccessible.

Examples

The following example creates a static terminal alias in the local zone:

```
zone local gk.zone1.com zone1.com
alias static 192.168.8.5 gkid gk.zone1.com terminal e164 14085551212 h323id terminal1
```

allow-connections

To allow connections between specific types of endpoints in a VoIP network, use the **allow-connections** command in voice service configuration mode. To refuse specific types of connections, use the **no** form of this command.

allow-connections *from-type* **to** *to-type*

no allow-connections *from-type* **to** *to-type*

Syntax Description

from-type	Originating endpoint type. The following choices are valid: • **h323**—H.323. • **sip**—Session Interface Protocol (SIP).
to	Indicates that the argument that follows is the connection target.
to-type	Terminating endpoint type. The following choices are valid: • **h323**—H.323. • **sip**—Session Interface Protocol (SIP).

Command Default

Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.3, and Earlier Releases

H.323-to-H.323 connections are enabled by default and cannot be changed, and POTS-to-any and any-to-POTS connections are disabled.

Cisco IOS Release 12.3(7)T and Later Releases

H.323-to-H.323 connections are disabled by default and can be changed, and POTS-to-any and any-to-POTS connections are enabled.

H.323-to-SIP Connections

H.323-to-SIP and SIP-to-H.323 connections are disabled by default, and POTS-to-any and any-to-POTS connections are enabled.

SIP-to-SIP Connections

SIP-to-SIP connections are disabled by default, and POTS-to-any and any-to-POTS connections are enabled.

Command Modes

Voice service configuration

Command History

Cisco IOS Release	Modification
12.2(13)T3	This command was introduced.
12.3(7)T	The default was changed.
12.3(11)T	The **sip** endpoint option was introduced for use with Cisco CallManager Express.

Cisco IOS Release	Modification
12.2(13)T3	This command was introduced.
12.4(4)T	The **sip** endpoint option was implemented for use in IP-to-IP gateway networks.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.3, and Earlier Releases

This command is used to allow connections between specific types of endpoints in a Cisco multiservice IP-to-IP gateway. The command is enabled by default and cannot be changed. Connections to or from POTS endpoints are not allowed. Only H.323-to-H.323 connections are allowed.

Cisco IOS Release 12.3(7)T and Later Releases

This command is used with Cisco Unified Communications Manager Express 3.1 or later systems and with the Cisco Multiservice IP-to-IP Gateway feature. In Cisco Unified Communications Manager Express, the **allow-connections** command enables the VoIP-to-VoIP connections used for hairpin call routing or routing to an H.450 tandem gateway.

Examples

The following example specifies that connections between H.323 and SIP endpoints are allowed:

```
Router(config-voi-serv)# allow-connections h323 to sip
```

The following example specifies that connections between H.323 endpoints are allowed:

```
Router(config-voi-serv)# allow-connections h323 to h323
```

The following example specifies that connections between SIP endpoints are allowed:

```
Router(config-voi-serv)# allow-connections sip to sip
```

Related Commands

Command	Description
voice service	Enters voice service configuration mode.

allow subscribe

To allow internal watchers to monitor external presentities, use the **allow subscribe** command in presence configuration mode. To disable external watching, use the **no** form of this command.

allow subscribe

no allow subscribe

Syntax Description

This command has no arguments or keywords.

Command Default

Only internal presentities can be watched when presence is enabled.

Command Modes

Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command allows internal watchers to receive Busy Lamp Field (BLF) status notification for external directory numbers on a remote router connected through a SIP trunk. An external directory number must be enabled as a presentity with the **allow watch** command.

The router sends SUBSCRIBE requests through the SIP trunk to an external presence server on behalf of the internal watcher and returns presence status to the watcher. To permit the external directory numbers to be watched, you must enable the **watcher all** command on the remote router.

Examples

The following example shows how to enable internal watchers to monitor external presentities:

```
Router(config)# presence
Router(config-presence)# allow subscribe
```

Related Commands

Command	Description
allow watch	Allows a line on a phone registered to Cisco Unified CME to be watched in a presence service.
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
presence	Enables presence service on the router and enters presence configuration mode.
presence call-list	Enables BLF monitoring for call lists and directories on phones registered to Cisco Unified CME.

Command	Description
presence enable	Allows incoming presence requests from SIP trunks.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows an external watcher to monitor an internal presentity.

alt-dial

To configure an alternate dial-out string for dial peers, use the **alt-dial** command in dial peer configuration mode. To delete the alternate dial-out string, use the **no** form of this command.

alt-dial *string*

no alt-dial *string*

Syntax Description

string	The alternate dial-out string.

Command Default No alternate dial-out string is configured

Command Modes Dial Peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines This command applies to plain old telephone service (POTS), Voice over Frame Relay (VoFR), and Voice ATM (VoATM) dial peers.

The **alt-dial** command is used for the on-net-to-off-net alternative dialing function. The string replaces the destination-pattern string for dialing out.

Examples The following example configures an alternate dial-out string of 95550188:

```
alt-dial 95550188
```

anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **anat** command in voice service voip-sip configuration mode or dial peer configuration mode. To ANAT on SIP trunks, use the **no** form of this command.

anat

no anat

Syntax Description This command has no arguments or keywords.

Command Default ANAT is enabled on SIP trunks.

Command Modes Voice service voip-sip configuration
Dial peer configuration

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines Both the Cisco IOS SIP gateway and the Cisco Unified Border Element are required to support Session Description Protocol (SDP) ANAT semantics for SIP IPv6 sessions. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IP versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped "m" lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

Examples The following example enables ANAT on a SIP trunk:

```
router(conf-serv-sip)# anat
```

ani mapping

To preprogram the Numbering Plan Area (NPA), or area code, into a single Multi Frequency (MF) digit, use the **ani mapping** command in voice-port configuration mode. To disable Automatic Number Identification (ANI) mapping, use the **no** form of this command.

ani mapping *npd-value npa-number*

no ani mapping

Syntax Description

npd-value	Value of the Numbering Plan Digit (NPD). Range is 0 to 3. There is no default.
npa-number	Number (area code) of the NPA. Range is 100 to 999. There is no default value.

Command Default No default behavior or values

Command Modes Voice-port configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines The **ani mapping** command table translates the NPA into a single MF digit. The number of NPDs programmed is determined by local policy as well as by the number of NPAs that the public service answering point (PSAP) serves. Repeat this command until all NPDs are configured or until the NPD maximum range is reached.

Examples The following example shows the voice port preprogramming the NPA into a single MF digit:

```
voice-port 1/1/0
 timing digit 100
 timing inter-digit 100
 ani mapping 1 408
 signal cama KP-NPD-NXX-XXXX-ST
!
voice-port 1/1/1
 timing digit 100
 timing inter-digit 100
 ani mapping 1 408
 signal cama KP-NPD-NXX-XXXX-ST
```

Related Commands

Command	Description
signal	Specifies the type of signaling for a CAMA port.
voice–port	Enters voice-port configuration mode.

answer-address

To specify the full E.164 telephone number to be used to identify the dial peer of an incoming call, use the **answer-address** command in dial peer configuration mode. To disable the configured telephone number, use the **no** form of this command.

answer-address [**+**]*string*[**T**]

no answer-address

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default The default value is enabled with a null string

Command Modes Dial peer voice configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines Use the **answer-address** command to identify the origin (or dial peer) of incoming calls from the IP network. Cisco IOS software identifies the dial peers of a call in one of two ways: by identifying either the interface through which the call is received or the telephone number configured with the **answer-address** command. In the absence of a configured telephone number, the peer associated with the interface is associated with the incoming call.

For calls that come in from a plain old telephone service (POTS) interface, the **answer-address** command is not used to select an incoming dial peer. The incoming POTS dial peer is selected on the basis of the port configured for that dial peer.

There are certain areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **answer-address** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

Note Cisco IOS software does not check the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples The following example shows the E.164 telephone number 555-0104 as the dial peer of an incoming call being configured:

```
dial-peer voice 10 pots
 answer-address +5550104
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
port (dial peer)	Associates a dial peer with a specific port.
prefix	Specifies the prefix of the dialed digits for a dial peer.

application (dial peer)

To enable a specific application on a dial peer, use the **application** command in dial peer configuration mode. To remove the application from the dial peer, use the **no** form of this command.

application *application-name* [**out-bound**]

no application *application-name* [**out-bound**]

Syntax Description

application-name	Name of the predefined application that you wish to enable on the dial peer. See the "Usage Guidelines" section for valid application names.
out-bound	(Optional) Outbound calls are handed off to the named application. This keyword is used for store-and-forward fax applications and VoiceXML applications.

Command Default No default behavior or values

Command Modes Dial peer voice configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.0(5)T	The SGCPAPP application was supported initially on the Cisco AS5300.
12.0(7)XK	Support for the SGCPAPP application was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620).
12.1(2)T	The SGCPAPP application was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	The MGCPAPP application was implemented on the Cisco AS5300.
12.1(3)XI	The **out-bound** keyword was added for store-and-forward fax on the Cisco AS5300.
12.1(5)T	The **out-bound** keyword was integrated into Cisco IOS Release 12.1(5)T, and the command was implemented on the Cisco AS5800.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(4)XM	This command was implemented on the Cisco 1751.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: The Cisco 3725 and Cisco 3745. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco CallManager Version 3.2 and implemented on the Cisco 1760 and Cisco IAD2420 series routers. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.2(13)T	The *application-name* argument was removed from the **no** form of this command.
12.2(15)T	Malicious Caller Identification (MCID) was added as a valid *application-name* argument.
12.2(15)ZJ	The session application referred to by the **default** value of the *application-name* argument was updated to include support for Open Settlement Protocol (OSP), call transfer, and call forwarding. The version of the session application referred to by **default** in Cisco IOS Release 12.2(13)T and earlier releases was renamed default.c.old.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(14)T	This command is obsolete in Cisco IOS Release 12.3(14)T. For Cisco IOS Release 12.3(14)T and later releases, use the **application** command in global configuration mode to configure applications on a dial peer.

Usage Guidelines

Use this command when configuring interactive voice response (IVR) or any of the IVR-related features to associate a predefined session application with an incoming POTS dial peer and an outgoing Multimedia Mail over IP (MMoIP) dial peer. Calls that use the incoming POTS dial peer and the outgoing MMoIP dial peer are handed off to the specified predefined session application.

Note In Cisco IOS Release 12.2(15)T and later releases, the application name default refers to the application new version of the default session application that supports OSP, call transfer, and call forwarding. The default session application in Cisco IOS Release 12.2(13)T and earlier releases has been renamed default.old.c and can still be configure for specific dial peers through the **application** command or globally configured for all inbound dial peers through the **call application global** command.

For Media Gateway Control Protocol (MGCP) and Simple Gateway Control Protocol (SGCP) networks, enter the application name in uppercase characters. For example, for MGCP networks, you would enter MGCPAPP for the *application-name* argument. The application can be applied only to POTS dial peers. Note that SGCP dial peers do not use dial-peer hunting.

Note In Cisco IOS Release 12.2, you cannot mix SGCP and non-SGCP endpoints in the same T1 controller, nor can you mix SGCP and non-SGCP endpoints in the same DS0 group.

Note MGCP scripting is not supported on the Cisco 1750 router or on Cisco 7200 series routers.

For H.323 networks, the application is defined by a Tool Command Language/interactive voice response (Tcl/IVR) filename and location. Incoming calls that use POTS dial peers and outgoing calls that use MMoIP dial peers are handed off to this application**.**

For Session Initiation Protocol (SIP) networks, use this command to associate a predefined session application. The default Tcl application (from the Cisco IOS image) for SIP is session and can be applied to both VoIP and POTS dial peers.

Examples

The following example defines an application and applies it to an outbound MMoIP dial peer for the fax on-ramp operation:

```
call application voice fax_on_vfc_onramp http://santa/username/clid_4digits_npw_3.tcl
dial-peer voice 3 mmoip
 application fax_on_vfc_onramp out-bound
 destination-pattern 57108..
 session target mailto:$d$@mail-server.cisco.com
```

The following example applies the MGCP application to a dial peer:

```
dial-peer voice 1 pots
 application MGCPAPP
```

The following example applies a predefined application to an incoming POTS dial peer:

```
dial-peer voice 100 pots
 application c4
```

The following example applies a predefined application to an outbound MMoIP dial peer for the on-ramp operation:

```
dial-peer voice 3 mmoip
  application fax_on_vfc_onramp_ap out-bound
  destination-pattern 57108..
  session target mailto:$d$@mail-server.cisco.com
```

The following example applies the predefined SIP application to a dial peer:

```
dial-peer voice 10 pots
 application session
```

For Cisco IOS Release 12.2(15)T, MCID was added as a valid *application-name* argument. The following is a sample configuration using the MCID application name:

```
call application voice mcid http://santa/username/app_mcid_dtmf.2.0.0.28.tcl
dial-peer voice 3 pots
 application mcid
 incoming called-number 222....
 direct-inward-dial
 port 1:D
```

Related Commands

Command	Description
application	Enables a specific application on a dial peer.
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
mgcp	Starts the MGCP daemon.
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

application (global)

To enter application configuration mode to configure applications, use the **application** command in global configuration mode.

application

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **application** command in dial peer configuration mode.

Usage Guidelines

Use this command to enter application configuration mode. Related commands are used in application configuration mode to configure standalone applications (services) and linkable functions (packages).

Examples

The following example shows how to enter application configuration mode and configure a debit card service:

Enter application configuration mode to configure applications and services:

```
Router(config)# application
```

Load the debit card script:

```
Router(config-app)# service debitcard
tftp://server-1/tftpboot/scripts/app_debitcard.2.0.2.8.tcl
```

Configure language parameters for the debit card service:

```
Router(config-app-param)# paramspace english language en
  paramspace english index 1
  paramspace english prefix en
  paramspace english location tftp://server-1/tftpboot/scripts/au/en/
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specify the location of the Tcl or VoiceXML document to load for this application.

arq reject-resource-low

To configure the gatekeeper to send an Admission Reject (ARJ) message to the requesting gateway if destination resources are low, use the **arq reject-resource-low** command in gatekeeper configuration mode. To disable the gatekeeper from checking resources, use the **no** form of this command.

arq reject-resource-low

no arq reject-resource-low

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows that the gatekeeper is configured to send an ARJ message to the requesting gateway if destination resources are low:

```
gatekeeper
 arq reject-resource-low
```

Related Commands

Command	Description
lrq reject-resource-low	Configures a gatekeeper to notify a sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available.

arq reject-unknown-prefix

To enable the gatekeeper to reject admission requests (ARQs) for zone prefixes that are not configured, use the **arq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming ARQs, use the **no** form of this command.

arq reject-unknown-prefix

no arq reject-unknown-prefix

Syntax Description

This command has no arguments or keywords

Command Default

The gatekeeper accepts and processes all incoming ARQs.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)Q,	This command was introduced.
11.3(7)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **arq reject-unknown-prefix** command to configure the gatekeeper to reject any incoming ARQs for a destination E.164 address that does not match any of the configured zone prefixes.

When an endpoint or gateway initiates an H.323 call, it sends an ARQ to its gatekeeper. The gatekeeper uses the configured list of zone prefixes to determine where to direct the call. If the called address does not match any of the known zone prefixes, the gatekeeper attempts to *hairpin* the call out through a local gateway. If you do not want your gateway to do this, then use the **arq reject-unknown-prefix** command. (The term *hairpin* is used in telephony. It means to send a call back in the direction from which it came. For example, if a call cannot be routed over IP to a gateway that is closer to the target phone, the call is typically sent back out through the local zone, back the way it came.)

This command is typically used to either restrict local gateway calls to a known set of prefixes or deliberately fail such calls so that an alternate choice on a gateway's rotary dial peer is selected.

Examples

Consider a gatekeeper configured as follows:

```
zone local gk408 cisco.com
zone remote gk415 cisco.com 172.21.139.91
zone prefix gk408 1408.......
zone prefix gk415 1415.......
```

In this example configuration, the gatekeeper manages a zone containing gateways to the 408 area code, and it knows about a peer gatekeeper that has gateways to the 415 area code. Using the **zone prefix** command, the gatekeeper is then configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

If the **arq request-unknown-prefix** command is not configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is routed to a local gateway in the gk408 zone.

If the **arq reject-unknown-prefix** command is configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is rejected because the destination address does not match any configured prefix.

Related Commands

Command	Description
zone prefix	Adds a prefix to the gatekeeper zone list.

as

To define an application server for backhaul, use the **as** command in IUA configuration mode. To disable the backhaul ability from an application server, use the **no** form of this command.

as *as-name* {*localip1* [*localip2*]} [**local-sctp-port**] [**fail-over-timer**] [**sctp-startup-rtx**] [**sctp-streams**] [**sctp-t1init**]

no as *name*

Syntax Description

as-name	Defines the protocol name (only ISDN is supported).
localip1	Defines the local IP address(es) for all the ASPs in a particular AS.
localip2	(Optional) Defines the local IP address(es) for all the ASPs in a particular application server .
local-sctp-port	(Optional) Defines a specific local Simple Control Transmission Protocol (SCTP) port rather than an ISDN Q.921 User Adaptation Layer (IUA) well-known port.
fail-over-timer	(Optional) Configures the failover timer for a particular application server .
sctp-startup-rtx	(Optional) Configures the SCTP maximum startup retransmission timer.
sctp-streams	(Optional) Configures the number of SCTP streams for a particular application server .
sctp-t1init	(Optional) Configures the SCTP T1 initiation timer.

Command Default No application server is defined.

Command Modes IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 platform.
12.2(13)T1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines A maximum of two local IP addresses can be specified. (Note that SCTP has built-in support for multihomed machines.)

Note All of the ASPs in an application server must be removed before an application server can be unconfigured.

The default value of the SCTP streams is determined by the hardware that you have installed. The value of the failover timer is found in the **show iua as all** command output.

The number of streams to assign to a given association is implementation dependent. During the initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple trunk group support, every interface can potentially be a separate D channel.

At startup, the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the gateway (GW) and the Media Gateway Controller (MGC). For the rare case that you are configuring multiple AS associations to various MGCs, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during startup, the IUA code adds one to the total number of interfaces (streams) found.

You have the option to manually configure the number of streams per association. In the backhaul scenario, if the number of D channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that is never used. For multiple associations between a GW and multiple MGCs, the configuration utility is useful in providing only the necessary number of streams per association. The overhead from the streams allocated but not used in the association is negligible.

If the number of streams is manually configured through the CLI, the IUA code cannot distinguish between a startup event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you are configuring the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword. Otherwise, IUA needs to always add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with the CLI, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA AS configuration and then configure it back as the same application server or a new one. The other option is to reload the router.

Examples

An application server and the application server process (ASP) should be configured first to allow a National ISDN-2 with Cisco extensions (NI2+) to be bound to this transport layer protocol. The application server is a logical representation of the SCTP local endpoint. The local endpoint can have more than one IP address but must use the same port number.

The following is an example of an application server configuration on a gateway. The configuration shows that an application server named as5400-3 is configured to use two local IP addresses and a port number of 2577:

```
Router(config-iua)# as as5400-3 10.1.2.34 10.1.2.35 2577
```

The following output shows that the application server (as1) is defined for backhaul:

```
AS as1 10.21.0.2 9900
```

Related Commands

Command	Description
asp	Defines an ASP for backhaul.

asp

To define an application server process (ASP) for backhaul, use the **asp** command in IUA configuration mode. To disable the ASP, use the **no** form of this command.

asp *asp-name* **as** *as-name* {*remoteip1* [*remoteip2*]} [**remote-sctp-port**] [**ip-precedence** [**sctp-keepalives**] [**sctp-max-associations**] [**sctp-path-retransmissions**] [**sctp-t3-timeout**]

no asp *asp-name*

Syntax Description

asp-name	Names the current ASP.
as	The application server to which the ASP belongs.
as-name	Name of the application server to which the ASP belongs.
remoteip1	(Optional) Designates the remote IP address for this Simple Control Transmission Protocol (SCTP) association.
remoteip2	Designates the remote IP address for this SCTP association.
remote-sctp-port	Connects to a remote SCTP port rather than the IUA well-known port.
ip-precedence	(Optional) Sets IP Precedence bits for protocol data units (PDUs). • IP precedence is expressed in the type of service (ToS) field of the **show ip sctp association parameters** output. The default type of service (ToS) value is 0. • Valid precedence values range from 0 to 7. You can also use the default IP precedence value for this address by choosing the default option.
sctp-keepalives	(Optional) Modifies the keepalive behavior of an IP address in a particular ASP. • Valid keepalive interval values range from 1000 to 60000. The default value is 500 ms (see the **show ip sctp association parameters** output under **heartbeats**).
sctp-max-associations	(Optional) Sets the SCTP maximum association retransmissions for a particular ASP. Valid values range from 2 to 20. The default is 5.
sctp-path-retransmissions	(Optional) Sets the SCTP path retransmissions for a particular ASP. Valid values range from 2 to 10. The default is 3.
sctp-t3-timeout	(Optional) Sets the SCTP T3 retransmission timeout for a particular ASP. The default value is 900 ms.

Command Default No ASP is defined.

Command Modes IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco AS5300.
12.2(11)T1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

This command establishes SCTP associations. There can be only a maximum of three ASPs configured per AS. IP precedence is expressed in the ToS field of **show ip sctp association parameters** output. The default ToS value is 0.

Note All of the ASPs in an application server must be removed before an application serever can be unconfigured.

You can configure the precedence value in IUA in the range of 0 to 7 for a given IP address. Within IUA, the upper three bits representing the IP precedence in the ToS byte (used in the IP header) is set based on the user input before passing down the value to SCTP. In turn, SCTP passes the ToS byte value to IP. The default value is 0 for "normal" IP precedence handling.

The *asp-name* argument specifies the name of this ASP. The **ip-precedence** keyword sets the precedence and ToS field. The *remote-ip-address* argument specifies the IP address of the remote end-point (the address of MGC, for example). The *number* argument can be any IP precedence bits in the range 1 to 255.

The **no** form of the command results in precedence bits not being explicitly set by SCTP.

In the case of a hot-standby Cisco PGW2200 pair, from the gateway (GW) perspective there is usually one ASP active and another in the INACTIVE state. The ASP_UP message is used to bring the ASP state on the GW to the INACTIVE state, followed by the ASPTM message, ASP_ACTIVE to ready the IUA link for data exchange. (Eventually the QPTM Establish Request message actually initiates the start of the D channel for the given interface.) In the event that the GW detects a failure on the active ASP, it can send a NTFY message to the standby ASP to request that it become active.

Examples

An ASP can be viewed as a local representation of an SCTP association because it specifies a remote endpoint that is in communication with an AS local endpoint. An ASP is defined for a given AS. For example, the following configuration defines a remote signaling controller *asp-name* at two IP addresses for AS as1. The remote SCTP port number is 2577:

```
Router(config-iua)# as as1 10.4.8.69, 10.4.9.69 2477
Router(config-iua)# asp asp1 as as1 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single AS for the purpose of redundancy, but only one ASP can be active. The ASPs are inactive and only become active after fail-over.

In the Cisco Media Gateway Controller (MGC) solution, a signaling controller is always the client that initiates the association with a gateway. During the initiation phase, you can request outbound and inbound stream numbers, but the gateway only allows a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The following example specifies the IP precedence level on the specified IP address. This example uses IP precedence level 7, which is the maximum level allowed:

```
Router(config-iua)# asp asp1 as ip-precedence 10.1.2.345 7
```

The following example specifies the IP address to enable and disable keepalives:

```
Router(config-iua)# asp asp1 as sctp-keepalive 10.1.2.34
```

The following example specifies the keepalive interval in milliseconds. In this example, the maximum value of 60000 ms is used:

```
Router(config-iua)# asp asp1 as sctp-keepalive 10.10.10.10 60000
```

The following example specifies the IP address for the SCTP maximum association and the maximum association value. In this example, a maximum value of 20 is used:

```
Router(config-iua)# asp asp1 as sctp-max-association 10.10.10.10 20
```

The following example specifies the IP address for the SCTP path retransmission and the maximum path retransmission value. In this example, a maximum value of 20 is used:

```
Router(config-iua)# asp asp1 as sctp-path-retransmissions 10.10.10.10 10
```

The following example specifies the IP address for SCTP T3 timeout and specifies the T3 timeout value in milliseconds. In this example, the maximum value of 60000 is used:

```
Router(config-iua)# asp asp1 as sctp-t3-timeout 10.10.10.10 60000
```

Related Commands

Command	Description
as	Defines an application server for backhaul.

asserted-id

To set the privacy level and enable either P-Asserted-Identity (PAI) or P-Preferred-Identity (PPI) privacy headers in outgoing SIP requests or response messages, use the **asserted-id** command in voice service voip-sip configuration mode or on a dial peer. To remove the privacy level of either PAI or PPI, use the **no** form of this command.

asserted-id [**pai** | **ppi**]

no asserted-id

Syntax Description

pai	(Optional) Enables PAI privacy headers in outgoing SIP requests or response messages.
ppi	(Optional) Enables PPI privacy headers in outgoing SIP requests or response messages.

Command Default

The command is disabled.

Command Modes

Voice service voip-sip configuration
Dial-peer configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Enter SIP configuration mode from voice-service configuration mode, as shown in the example.

If you configure the **asserted-id pai** command, the gateway builds a P-Asserted-Identity header into the common SIP stack. The **asserted-id pai** command has a priority over the Remote-Party-ID (RPID) header and removes this header from any outbound message, even if the router is configured to use the RPID header.

If you configure the **asserted-id ppi** command, the gateway builds a P-Preferred-Identity header into the common SIP stack. The **asserted-id ppi** command has a priority over the Remote-Party-ID (RPID) header and removes this header from any outbound message, even if the router is configured to use the RPID header.

Examples

The following example shows how to set the P-Asserted Identity in the privacy header:

```
router> enable
router# configure terminal
router(config)# voice service voip
router(conf-voi-serv)# sip
router(conf-serv-sip)# asserted-id pai
```

Related Commands

Command	Description
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.
privacy	Sets privacy in support of RFC 3323.

associate application

To associate an application to the digital signal processor (DSP) farm profile, use the **associate application** command in DSP farm profile configuration mode. To remove the protocol, use the **no** form of this command.

associate application {**cube** | **sbc** | **sccp**} *profile-description-text*

no associate application sccp

Syntax Description

cube	Associates the Cisco Unified Border Element application to a defined profile in the DSP farm.
sbc	Associates the SBC application to a defined profile in the DSP farm.
sccp	Associates the skinny client control protocol application to a defined profile in the DSP farm.
profile-description-text	(Optional) User defined name for the associated applicaion.

Command Default No application is associated with the DSP farm profile.

Command Modes DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was modified. The **cube** and **sbc** keywords and the *profile-description-text* argument were added.

Usage Guidelines Use the associate application command to associate an application to a predefinded DSP farm profile.

Examples The following example associates SCCP to the DSP farm profile:

```
Router(config-dspfarm-profile)# associate application sccp
```

The following example associates Cisco Unified Border Element to the DSP farm profile:

```
Router(config-dspfarm-profile)# associate application cube
```

Related Commands

Command	Description
voice-card	Enters voice card configuration mode
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.
shutdown (dspfarm-profile)	Allocates DSP farm resources and associates with the application.

associate ccm

To associate a Cisco Unified CallManager with a Cisco CallManager group and establish its priority within the group, use the **associate ccm** command in the SCCP Cisco CallManager configuration mode. To disassociate a Cisco Unified CallManager from a Cisco CallManager group, use the **no** form of this command.

associate ccm *identifier-number* **priority** *priority-number*

no associate ccm *identifier-number* **priority** *priority-number*

Syntax Description

identifier-number	Number that identifies the Cisco Unified CallManager. Range is 1 to 65535. There is no default value.
priority *priority-number*	Priority of the Cisco Unified CallManager within the Cisco CallManager group. Range is 1 to 4. There is no default value. The highest priority is 1.

Command Default

No default behavior or values

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example associates Cisco Unified CallManager 125 with Cisco CallManager group 999 and sets the priority of the Cisco Unified CallManager within the group to 2:

```
Router(config)# sccp ccm group 999
Router(config-sccp-ccm)# associate ccm 125 priority 2
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager connections fails.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.

associate profile

To associate a digital signal processor (DSP) farm profile with a Cisco CallManager group, use the **associate profile** command in SCCP Cisco CallManager configuration mode. To disassociate a DSP farm profile from a Cisco Unified CallManager, use the **no** form of this command.

associate profile *profile-identifier* **register** *device-name*

no associate profile *profile-identifier* **register** *device-name*

Syntax Description

profile-identifier	Number that identifies the DSP farm profile. Range is 1 to 65535. There is no default value.
register *device-name*	User-specified device name in Cisco Unified CallManager. A maximum number of 15 characters can be entered for the device name.

Command Default This command is not enabled.

Command Modes SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines The device name must match the name configured in Cisco UnifiedCallManager; otherwise the profile is not registered to Cisco Unified CallManager.

Note Each profile can be associated to only one Cisco CallManager group.

Examples The following example associates DSP farm profile abgz12345 to Cisco CallManager group 999:

```
Router(config)# sccp ccm group 999
Router(conif-sccp-ccm)# associate profile 1 register abgz12345
```

Related Commands

Command	Description
bind interface	Binds an interface to a Cisco CallManager group.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm group	Creates a Cisco CallManager group and enters SCCP Cisco CallManager configuration mode.

associate registered-number

To associate the preloaded route and outbound proxy details with the registered number, use the **associate registered-number** command in voice service VoIP SIP configuration mode. To remove the association, use the **no** form of this command.

associate registered-number *number*

no associate registered-number

Syntax Description

number	Registered number. The number must be between 4 and 32.

Command Default The preloaded route and outbound proxy details are not associated with the registered number by default.

Command Modes Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Examples The following example shows how to associate a registered number in the SIP configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# associate registered-number 5
```

Related Commands

Command	Description
voice-class sip associate registered-number	Associates preloaded route and outbound proxy details with the registered number in the dial-peer configuration level.

asymmetric payload

To configure Session Initiation Protocol (SIP) asymmetric payload support, use the **asymmetric payload** command in SIP configuration mode. To disable asymmetric payload support, use the **no** form of this command.

asymmetric payload {**dtmf** | **dynamic-codecs** | **full** | **system**}

no asymmetric payload

Syntax Description

dtmf	(Optional) Specifies that the asymmetric payload support is dual-tone multi-frequency (DTMF) only.
dynamic-codecs	(Optional) Specifies that the asymmetric payload support is for dynamic codec payloads only.
full	(Optional) Specifies that the asymmetric payload support is for both DTMF and dynamic codec payloads.
system	(Optional) Specifies that the asymmetric payload uses the global value.

Command Default This command is disabled.

Command Modes Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS Release IOS XE 3.1.

Usage Guidelines Enter SIP configuration mode from voice-service configuration mode, as shown in the example.

For the Cisco UBE the SIP asymmetric payload-type is supported for audio/video codecs, DTMF, and NSE. Hence, **dtmf** and **dynamic-codecs** keywords are internally mapped to the **full** keyword to provide asymmetric payload-type support for audio/video codecs , DTMF, and NSE.

Examples The following example shows how to set up a full asymmetric payload globally on a SIP network for both DTMF and dynamic codecs:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# asymmetric payload full
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip asymmetric payload	Configures SIP asymmetric payload support on a dial peer.

atm scramble-enable

To enable scrambling on E1 links, use the **atm scramble-enable** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

atm scramble-enable

no atm scramble-enable

Syntax Description This command has no arguments or keywords.

Command Default By default, payload scrambling is set off

Command Modes Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines Enable scrambling on E1 links only. On T1 links, the default binary 8-zero substitution (B8ZS) line encoding normally ensures sufficient reliability. Scrambling improves data reliability on E1 links by randomizing the ATM cell payload frames to avoid continuous nonvariable bit patterns and to improve the efficiency of the ATM cell delineation algorithms.

The scrambling setting must match that of the far end.

Examples The following example shows how to set the ATM0 E1 link to scramble payload:

```
interface atm0
 atm scramble-enable
```

atm video aesa

To set the unique ATM end-station address (AESA) for an ATM video interface that is using switched virtual circuit (SVC) mode, use the **atm video aesa** command in ATM interface configuration mode. To remove any configured address for the interface, use the **no** form of this command.

atm video aesa [**default** | *esi-address*]

no atm video aesa

Syntax Description

default	(Optional) Automatically creates a network service access point (NSAP) address for the interface, based on a prefix from the ATM switch (26 hexadecimal characters), the MAC address (12 hexadecimal characters) as the end station identifier (ESI), and a selector byte (two hexadecimal characters).
esi-address	(Optional) Defines the 12 hexadecimal characters used as the ESI. The ATM switch provides the prefix (26 hexadecimal characters), and the video selector byte provides the remaining two hexadecimal characters.

Command Default **default**

Command Modes ATM Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines You cannot specify the ATM interface NSAP address in its entirety. The system creates either all of the address or part of it, depending on how you use this command.

Examples The following example shows the ATM interface NSAP address set automatically:

```
interface atm0
 atm video aesa default
```

The following example shows the ATM interface NSAP address set to a specific ESI value:

```
interface atm0/1
 atm video aesa 444444444444
```

Related Commands

Command	Description
show atm video-voice address	Displays the NSAP address for the ATM interface.

attribute acct-session-id overloaded

To overload the acct-session-id attribute with call detail records, use the **attribute acct-session-id overloaded** command in gateway accounting AAA configuration mode. To disable overloading the acct-session-id attribute with call detail records, use the **no** form of this command.

attribute acct-session-id overloaded

no attribute acct-session-id overloaded

Syntax Description

This command has no arguments or keywords.

Command Default

The acct-session-id attribute is not overloaded with call detail records.

Command Modes

Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

- The **attribute acct-session-id overloaded** command replaces the **gw-accounting h323** command.
- The acct-session-id attribute is RADIUS attribute 44. For more information on this attribute, see the document *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.
- Attributes that cannot be mapped to standard RADIUS attributes are packed into the acct-session-id attribute field as ASCII strings separated by the forward slash ("/") character.
- The Accounting Session ID (acct-session-id) attribute contains the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. This unique identifier makes it easy to match start and stop records in a log file.
- Accounting Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Examples

The following example shows the acct-session-id attribute being overloaded with call detail records:

```
gw-accounting aaa
 attribute acct-session-id overloaded
```

Related Commands

Command	Description
call accounting-template voice	Defines and loads the template file at the location defined by the URL.
gw-accounting aaa	Enables VoIP gateway accounting.

attribute h323-remote-id resolved

To resolve the h323-remote-id attribute, use the **attribute h323-remote-id resolved** command in gateway accounting AAA configuration mode. To keep the h323-remote-id attribute unresolved, use the **no** form of this command.

attribute h323-remote-id resolved

no attribute h323-remote-id resolved

Syntax Description This command has no arguments or keywords.

Command Default The h323-remote-id attribute is not resolved.

Command Modes gateway accounting aaa configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines In Cisco IOS Release 12.2(11)T, the **attribute h323-remote-id resolved** command replaces the **gw-accounting h323 resolve** command, and the h323-remote-id attribute has been added as a Cisco vendor-specific attribute (VSA). This attribute is a string that indicates the Domain Name System (DNS) name or locally defined host name of the remote gateway.

You can obtain the value of the h323-remote-id attribute by doing a DNS lookup of the h323-remote-address attribute. The h323-remote-address attribute indicates the IP address of the remote gateway.

Examples The following example sets the h323-remote-id attribute to resolved:

```
gw-accounting aaa
 attribute h323-remote-id resolved
```

Related Commands

Command	Description
gw-accounting aaa	Enables VoIP gateway accounting.

audio

To enable the incoming and outgoing IP-IP call gain/loss feature for audio volume control on the incoming dial peer and the outgoing dial peer, enter the **audio** command in dial-peer configuration mode. To disable this feature, use the **no** form of this command.

audio {**incoming** | **outgoing**} **level adjustment** *value*

no audio {**incoming** | **outgoing**} **level adjustment** *value*

Syntax Description

incoming	Enables the incoming IP-IP call volume control on either the incoming dial peer or the outgoing dial peer.
outgoing	Enables the outgoing IP-IP call volume control on either the incoming dial peer or the outgoing dial peer.
value	Range is -27 to 16.

Command Default This command is disabled by default, and there is no volume control available.

Command Modes Dial-peer configuration (config-dialpeer)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines This feature enables the adjustment of the audio volume within a Cisco Unified Border Element (Cisco UBE) call. As with codec repacketization, dissimilar networks that have different built-in loss/gain characteristics may experience connectivity problems. By adding the ability to control the loss/gain within the Cisco UBE, you can more easily connect your networks.

The DSP requires one level for each stream, so the *value* for audio incoming level-adjustment and the *value* for audio outgoing level-adjustment will be added together. If the combined values are outside of the limit the DSP can perform, the value sent to the DSP will be either the minimum (-27) or maximum (+16) supported by the DSP.

Caution For gain/loss control, be aware that adding gain in a network with echo can generate feedback loud enough to cause hearing damage. Always exercise extreme caution when configuring gain into your network.

To configure IP-IP Call Gain/Loss Control on a voice gateway, you must configure the incoming and outgoing VoIP dial peers.

Examples

The following example shows how to configure audio incoming level to 5 and the audio outgoing level to -5:

```
Router(config-dialpeer)# audio incoming level-adjustment 5
Router(config-dialpeer)# audio outgoing level-adjustment -5
```

Related Commands

Command	Description
show dial peer voice	Displays the codec setting for dial peers.

audio-prompt load

To initiate loading the selected audio file (.au), which contains the announcement prompt for the caller, from Flash memory into RAM, use the **audio-prompt load** command in privileged EXEC mode. This command does not have a **no** form.

audio-prompt load *name*

Syntax Description

name	Location of the audio file that you want to have loaded from memory, flash memory, an FTP server, an HTTP server, or an HTTPS (HTTP over Secure Socket Layer (SSL)) server.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced. **Note** With Cisco IOS Release 11.3(6)NA2, the URL pointer refers to the directory where Flash memory is stored.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. Support for other Cisco platforms is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.4(15)T	The *name* argument was modified to accept an HTTPS server URL.

Usage Guidelines The first time the interactive voice response (IVR) application plays a prompt, it reads it from the URL (or the specified location for the .au file, such as Flash or FTP) into RAM. Then it plays the script from RAM. An example of the sequence of events follows:

- When the first caller is asked to enter the account and personal identification numbers (PINs), the enter_account.au and enter_pin.au files are loaded into RAM from Flash memory.
- When the next call comes in, these prompts are played from the RAM copy.
- If all callers enter valid account numbers and PINs, the auth_failed.au file is not loaded from Flash memory into RAM.

The router loads the audio file only when the script initially plays that prompt after the router restarts. If the audio file is changed, you must run this privileged EXEC command to reread the file. This generates an error message if the file is not accessible or if there is a format error.

Examples

The following example shows how to load the enter_pin.au audio file from Flash memory into RAM:

```
audio-prompt load flash:enter_pin.au
```

The following example shows how to load the hello.au audio file from an HTTPS server into RAM:

```
audio-prompt load https://http-server1/audio/hello.au
```

authenticate redirecting-number

To enable a Cisco IOS voice gateway to authenticate and pass Session Initiation Protocol (SIP) credentials based on the redirecting number when available instead of the calling number of a forwarded call, use the **authenticate redirecting-number** command in voice service SIP configuration mode. To return a Cisco IOS voice gateway to the default setting so that the gateway uses only the calling number for SIP credentials, use the **no** form of this command.

authenticate redirecting-number

no authenticate redirecting-number

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco IOS voice gateway uses only the calling number of a forwarded call for SIP credentials even when the redirecting number information is available for that call.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When an INVITE message sent out by the gateway is challenged, it must respond with the appropriate SIP credentials before the call is established. The default global behavior for the gateway is to authenticate and pass SIP credentials based on the calling number and all dial peers on a gateway default to the global setting. However, for forwarded calls, it is sometimes more appropriate to use the redirecting number and this can be specified at either the global or dial peer level (configuring behavior for a specific dial peer supersedes the global setting).

Use the **authenticate redirecting-number** command in voice service SIP configuration mode to globally enable a Cisco IOS voice gateway to authenticate and pass SIP credentials based on the redirecting number when available. Use the **no** form of this command to configure the gateway to authenticate and pass SIP credentials based only on the calling number of forwarded calls unless otherwise configured at the dial peer level:

- Use the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode to supersede global settings and force a specific dial peer on the gateway to authenticate and pass SIP credentials based on the redirecting number when available.
- Use the **no** form of the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode to supersede global settings and force a specific dial peer on the gateway to authenticate and pass SIP credentials based only on the calling number regardless of the global setting.

The redirecting number is present only in the headers of forwarded calls. When this command is disabled or the redirecting number is not available (nonforwarded calls), the gateway uses the calling number for SIP credentials.

Examples

The following example shows how to globally enable a Cisco IOS voice gateway to authenticate and pass the redirecting number of a forwarded call when a SIP INVITE message is challenged:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# authenticate redirecting-number
```

Related Commands

Command	Description
voice-class sip authenticate redirecting-number	Supersedes global settings and enables a dial peer on a Cisco IOS voice gateway to authenticate and pass SIP credentials based on the redirecting number of forwarded calls.

authentication (dial peer)

To enable SIP digest authentication on an individual dial peer, use the **authentication** command in dial peer voice configuration mode. To disable SIP digest authentication, use the **no** form of this command.

authentication username *username* **password** [**0** | **7**] *password* [**realm** *realm* [**challenge**]]

no authentication username *username* [**password** [**0** | **7**] *password* [**realm** *realm* [**challenge**]]]

Syntax Description

username	Specifies the username for the user who is providing authentication.
username	A string representing the username for the user who is providing authentication. A username must be at least four characters.
password	Specifies password settings for authentication.
0	(Optional) Specifies encryption type as cleartext (no encryption). This is the default.
7	(Optional) Specifies encryption type as encrypted.
password	A string representing the password for authentication. If no encryption type is specified, the password will be cleartext format. The string must be between 4 and 128 characters.
realm	(Optional) Specifies the domain where the credentials are applicable.
realm	(Optional) A string representing the domain where the credentials are applicable.

Command Default

SIP digest authentication is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.1(3)T	This command was modified. The **challenge** keyword was added.

Usage Guidelines

The following configuration rules are applicable when enabling digest authentication:

- Only one username can be configured per dial peer. Any existing username configuration must be removed before configuring a different username.
- A maximum of five *password* or *realm* arguments can be configured for any one username.

  The *username* and *password* arguments are used to authenticate a user. An authenticating server/proxy issuing a 407/401 challenge response includes a realm in the challenge response and the user provides credentials that are valid for that realm. Because it is assumed that a maximum of five proxy servers in the signaling path can try to authenticate a given request from a user-agent client (UAC) to a user-agent server (UAS), a user can configure up to five password and realm combinations for a configured username.

Note The user provides the password in plain text but it is encrypted and saved for 401 challenge response. If the password is not saved in encrypted form, a junk password is sent and the authentication fails.

- The realm specification is optional. If omitted, the password configured for that username applies to all realms that attempt to authenticate.
- Only one password can be configured at a time for all configured realms. If a new password is configured, it overwrites any previously configured password.

  This means that only one global password (one without a specified realm) can be configured. If you configure a new password without configuring a corresponding realm, the new password overwrites the previous one.
- If a realm is configured for a previously configured username and password, that realm specification is added to that existing username and password configuration. However, once a realm is added to a username and password configuration, that username and password combination is valid only for that realm. A configured realm cannot be removed from a username and password configuration without first removing the entire configuration for that username and password—you can then reconfigure that username and password combination with or without a different realm.
- In an entry with both a password and realm, you can change either the password or realm.

Examples

The following example shows how to enable the digest authentication:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 pots
Router(config-dial-peer)# authentication username MyUser password 7 MyPassword realm
MyRealm.example.com
```

The following example shows how to remove a previously configured digest authentication:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 pots
Router(config-dial-peer)# no authentication username MyUser password MyPassword
```

Related Commands

Command	Description
authentication (SIP UA)	Enables SIP digest authentication globally.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS local hostname in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS local hostname in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

authentication (SIP UA)

To enable SIP digest authentication, use the **authentication** command in SIP UA configuration mode. To disable SIP digest authentication, use the **no** form of this command.

authentication username *username* **password** [**0** | **7**] *password* [**realm** *realm*]

no authentication username *username* [**password** [**0** | **7**] *password* [**realm** *realm*]]

Syntax Description

username *username*	A string representing the username for the user who is providing authentication (must be at least four characters).
password	Specifies password settings for authentication.
0	(Optional) Specifies encryption type as cleartext (no encryption). This is the default.
7	(Optional) Specifies encryption type as encrypted.
password	A string representing the password for authentication. If no encryption type is specified, the password will be cleartext format. The string must be between 4 and 128 characters.
realm *realm*	(Optional) A string representing the domain where the credentials are applicable.

Command Default

SIP digest authentication is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The following configuration rules are applicable when enabling digest access authentication:

- Only one username can be configured globally in SIP UA configuration mode. Any existing username configuration must be removed before configuring a different username.
- A maximum of five *password* or *realm* arguments are allowed for a given *username* argument.

  The *username* and *password* arguments are used to authenticate a user. An authenticating server/proxy issuing a 407/401 challenge response includes a realm in the challenge response and the user provides credentials that are valid for that realm. Because it is assumed that a maximum of five proxy servers in the signaling path can try to authenticate a given request from a user-agent client (UAC) to a user-agent server (UAS), a user can configure up to five password and realm combinations for a configured username.
- The realm specification is optional. If omitted, the password configured for that username applies to all realms that attempt to authenticate.

- Only one password can be configured at a time for all configured realms. If a new password is configured, it overwrites any previously configured password.

  This means that only one global password (one without a specified realm) can be configured. If you configure a new password without configuring a corresponding realm, the new password overwrites the previous one.
- If a realm is configured for a previously configured username and password, that realm specification is added to that existing username and password configuration. However, once a realm is added to a username and password configuration, that username and password combination is valid only for that realm. A configured realm cannot be removed from a username and password configuration without first removing the entire configuration for that username and password—you can then reconfigure that username and password combination with or without a different realm.
- In an entry with both a password and realm, you can change either the password or realm.

Examples

The following example shows how to enable digest access authentication:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# authentication username MyUser password MyPassword realm
example.com
```

The following example shows how to remove a previously configured digest access authentication:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# no authentication username MyUser password MyPassword realm
example.com
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

authentication method

To set an authentication method at login for calls that come into a dial peer, use the **authentication method** command in voice class AAA configuration mode. To disable the authentication method set at login, use the **no** form of this command.

authentication method *MethListName*

no authentication method *MethListName*

Syntax Description

MethListName	Authentication method list name.

Command Default

When this command is not used to specify a login authentication method, the system uses the **aaa authentication login h323** command as the default.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

This command is used to direct authentication requests to a RADIUS server based on dialed number information service (DNIS) or trunk grouping.

This command is used for directing dial-peer-based authentication requests. The method list must be defined during initial authentication setup.

Examples

In the example below, “dp” is the method list name used for authentication. The method list name is defined during initial authentication setup.

```
voice class aaa 1
 authentication method dp
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

authorization method

To set an authorization method at login for calls that are into a dial peer, use the **authorization method** command in voice class AAA configuration mode. To disable the authorization method set at login, use the **no** form of this command.

authorization method *MethListName*

no authorization method *MethListName*

Syntax Description

MethListName	Defines an authorization method list name.

Command Default

When this command is not used to specifiy a login authorization method, the system uses the **aaa authorization exec h323** command as the default.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

This command is used to direct authentication requests to a RADIUS server based on dialed number information service (DNIS) or trunk grouping.

This command is used for directing dial-peer-based authentication requests. The method list must be defined during initial authentication setup.

Examples

The following example set an authorization method of “dp”:

```
voice class aaa 1
 authorization method dp
```

Related Commands

Command	Description
aaa authorization exec	Runs authorization to determine if the user is allowed to run an EXEC shell.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

auto-config

To enable auto-configuration or to enter auto-config application configuration mode for the Skinny Client Control Protocol (SCCP) application, use the **auto-config** command in global configuration mode. To disable auto-configuration, use the **no** form of this command.

auto-config [**application sccp**]

no auto-config

Syntax Description

application sccp	(Optional) Enters auto-config application configuration mode for the SCCP application.

Command Default

Auto-configuration is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module for the SCCP application.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **auto-config** command used to enter auto-configuration application configuration mode for the SCCP application and the **no shutdown** command used to enable the SCCP application for download:

```
Router(config)# auto-config application sccp
Router(auto-config-app)# no shutdown
```

Related Commands

Command	Description
shutdown (auto-config application)	Disables an auto-configuration application for download.
show auto-config	Displays the current status of auto-configuration applications.

auto-cut-through

To enable call completion when a PBX does not provide an M-lead response, use the **auto-cut-through** command in voice-port configuration mode. To disable the auto-cut-through operation, use the **no** form of this command.

auto-cut-through

no auto-cut-through

Syntax Description

This command has no arguments or keywords.

Command Default

Auto-cut-through is enabled.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was first supported on the Cisco 2600 and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **auto-cut-through** command applies to ear and mouth (E&M) voice ports only.

Examples

The following example shows enabling of call completion on a router when a PBX does not provide an M-lead response:

```
voice-port 1/0/0
 auto-cut-through
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

Cisco IOS Voice Commands: B

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

backhaul-session-manager

To enter backhaul session manager configuration mode, use the **backhaul-session-manager** command in global configuration mode.

backhaul-session-manager

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was implemented on Cisco IAD2420. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use the **backhaul-session-manager** command to switch to backhaul session manager configuration mode from global configuration mode. Use the **exit** command to exit backhaul session manager configuration mode and return to global configuration mode.

Examples

The following example enters backhaul session manager configuration mode:

```
Router(config)# backhaul-session-manager
Router(config-bsm)#
```

Related Commands

Command	Description
clear backhaul-session-manager group	Resets the statistics or traffic counters for a specified session group.
clear rudpv1 statistics	Clears the RUDP statistics and failure counters.

Command	Description
group	Creates a session group and associates it with a specified session set.
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures maximum cumulative acknowledgments.
group out-of-sequence	Configures maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures maximum receive segments.
group retransmit	Configures maximum retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.
isdn bind-l3	Configures the ISDN serial interface for backhaul.
session group	Associates a transport session with a specified session group.
set	Creates a fault-tolerant or non-fault-tolerant session set with the client or server option.
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session groups.
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.
show backhaul-session-manager set	Displays session groups associated with a specific or all session sets.
show rudpv1	Displays RUDP statistics.

bandwidth (dial peer)

To set the maximum bandwidth on a POTS dial peer for an H.320 call, use the **bandwidth** command in dial peer configuration mode. To remove the bandwidth setting, use the **no** form of this command.

bandwidth maximum *value* [**maximum** *value*]

no bandwidth

Syntax Description

maximum *value*	Sets the maximum bandwidth for an H.320 call on a POTS dial peer. The range is 64 to 1024, entered in increments of 64 kilobits per second (kbps). The default is 64.
minimum *value*	(Optional) Sets the minimum bandwidth. Acceptable values are 64 kbps or **minimum** *value*=**maximum** *value*.

Command Default No maximum bandwidth is set.

Command Modes Dial peer configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to set the maximum and minimum bandwidth for an H.320 POTS dial-peer. Only the maximum bandwidth is required. The value must be entered in increments of 64 kbps. The minimum bandwidth setting is optional, and the value must be either 64 kbps or equal to the maximum value setting.

Examples The following example shows configuration for POTS dial peer 200 with a maximum bandwidth of 1024 kbps:

```
dial-peer voice 200 pots
 bandwidth maximum 1024
```

The following example shows configuration for POTS dial peer 11 with a maximum bandwidth of 640 and a minimum of 64:

```
dial-peer voice 11 pots
 bandwidth maximum 640 minimum 64
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic and verifies the available bandwidth of the destination gatekeeper.

bandwidth

To specify the maximum aggregate bandwidth for H.323 traffic and verify the available bandwidth of the destination gatekeeper, use the **bandwidth** command in gatekeeper configuration mode. To disable maximum aggregate bandwidth, use the **no** form of this command.

bandwidth {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size*

no bandwidth {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*}

Syntax Description

interzone	Total amount of bandwidth for H.323 traffic from the zone to any other zone.
total	Total amount of bandwidth for H.323 traffic allowed in the zone.
session	Maximum bandwidth allowed for a session in the zone.
default	Default value for all zones.
zone	A particular zone.
zone-name	Name of the particular zone.
bandwidth-size	Maximum bandwidth, in kbps. For **interzone** and **total**, range : 1 to 10000000. For **session**, range:1 to 5000.

Command Default

Maximum aggregate bandwidth is unlimited by default.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500, Cisco 3600 series and the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. The **bandwidth** command replaced the **zone bw** command.
12.1(5)XM	The **bandwidth** command was recognized without using the **zone gatekeeper** command.
12.2(2)T	The changes in Cisco IOS Release 12.1(5)XM were integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command, in conjunction with the **bandwidth remote** command, replaces the **zone gatekeeper** command.

To specify maximum bandwidth for traffic between one zone and any other zone, use the **default** keyword with the **interzone** keyword.

To specify maximum bandwidth for traffic within one zone or for traffic between that zone and another zone (interzone or intrazone), use the **default** keyword with the **total** keyword.

To specify maximum bandwidth for a single session within a specific zone, use the **zone** keyword with the **session** keyword.

To specify maximum bandwidth for a single session within any zone, use the **default** keyword with the **session** keyword.

Examples

The following example configures the default maximum bandwidth for traffic between one zone and another zone to 5000 kbps:

```
gatekeeper
 bandwidth interzone default 5000
```

The following example configures the default maximum bandwidth for all zones to 5000 kbps:

```
gatekeeper
 bandwidth total default 5000
```

The following example configures the default maximum bandwidth for a single session within any zone to 2000 kbps:

```
gatekeeper
 bandwidth session default 2000
```

The following example configures the default maximum bandwidth for a single session with a specific zone to 1000 kbps:

```
gatekeeper
 bandwidth session zone example 1000
```

Related Commands

Command	Description
bandwidth check-destination	Enables the gatekeeper to verify available bandwidth resources at the destination endpoint.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines on which port the proxy listens.
h323 t120	Enables the T.120 capabilities on the router and specifies bypass or proxy mode.

bandwidth check-destination

To enable the gatekeeper to verify available bandwidth resources at the destination endpoint, use the **bandwidth check-destination command in** gatekeeper configuration mode. To disable resource verification, use the **no** form of this command.

bandwidth check-destination

no bandwidth check-destination

Syntax Description This command has no arguments or keywords.

Command Default Resource verification is disabled by default.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples The following example activates bandwidth resource verification at the destination:

```
gatekeeper
 bandwidth check-destination
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines the port on which port the proxy listens.
h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

bandwidth remote

To specify the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper, use the **bandwidth remote** command in gatekeeper configuration mode. To disable total bandwidth specified, use the **no** form of this command.

bandwidth remote *bandwidth-size*

no bandwidth remote

Syntax Description

bandwidth-size	Maximum bandwidth, in kbps. Range: 1 to 10000000.

Command Default

Total bandwidth is unlimited by default.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command, with the **bandwidth** command, replaces the **zone gatekeeper** command.

Examples

The following example configures the remote maximum bandwidth to 100,000 kbps:

```
gatekeeper
 bandwidth remote 100000
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth check-destination	Enables the gatekeeper to verify available bandwidth resources at the destination endpoint.
h323 interface	Defines which port the proxy listens on.
h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

battery-reversal

To specify battery polarity reversal on a Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) port, use the **battery-reversal command in** voice-port configuration mode. To disable battery reversal, use the **no** form of this command.

battery-reversal [**answer**]

no battery-reversal [**answer**]

Syntax Description

answer	(Optional) Configures an FXO port to support answer supervision by detection of battery reversal.

Command Default Battery reversal is enabled

Command Modes Voice-port configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series and Cisco 3600 series and on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	The **answer** keyword was added.

Usage Guidelines The **battery-reversal** command applies to FXO and FXS voice ports. On Cisco 2600 and 3600 series routers, only analog voice ports in VIC-2FXO-M1 and VIC-2FXO-M2 voice interface cards are able to detect battery reversal; analog voice ports in VIC-2FXO and VIC-2FXO-EU voice interface cards do not detect battery reversal. On digital voice ports, battery reversal is supported only on E1 Mercury Exchange Limited Channel Associated Signaling (MEL CAS); it is not supported in T1 channel associated signaling (CAS) or E1 CAS.

FXS ports normally reverse battery upon call connection. If an FXS port is connected to an FXO port that does not support battery reversal detection, you can use the **no battery-reversal** command on the FXS port to prevent unexpected behavior.

FXO ports in loopstart mode normally disconnect calls when they detect a second battery reversal (back to normal). You can use the **no battery-reversal** command on FXO ports to disable this action.

The **battery-reversal** command restores voice ports to their default battery-reversal operation.

If an FXO voice port is connected to the PSTN and supports battery reversal, use the **battery-reversal** command with the **answer** keyword to configure answer supervision. This configures the FXO voice port to detect when a call is answered in order to provide correct billing information.

If the voice port, PSTN, or PBX does not support battery reversal, do not use the **battery-reversal** command because it prevents outgoing calls from being connected. Use the **supervisory answer dualtone** command instead.

If an FXO port or its peer FXS port does not support battery reversal, avoid configuring **battery-reversal** or **battery-reversal answer** on the FXO port. On FXO ports that do not support battery reversal, the **battery-reversal** command can cause unpredictable behavior, and the **battery-reversal answer** command prevents calls from being answered. To ensure that battery reversal answer is disabled on FXO ports that do not support battery reversal, use the **no battery-reversal** command.

Examples

The following example disables battery reversal on voice port 1/0/0 on a router:

```
voice-port 1/0/0
 no battery-reversal
```

The following example enables battery reversal to provide answer supervision on voice port 1/0/0 on a router:

```
voice-port 1/0/0
 battery-reversal answer
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.
supervisory answer dualtone	Enables answer supervision on an FXO voice port on which battery reversal is not supported.

bearer-capability clear-channel

To specify the information transfer capability of the bearer capability information element (IE) in the outgoing ISDN SETUP message for Session Initiation Protocol (SIP) early-media calls that negotiate the clear-channel codec, use the **bearer-capability clear-channel** command in SIP configuration mode. To reset the information transfer capability of the bearer capability IE to **speech** (default), use the **no** form of this command.

bearer-capability clear-channel {**speech** | **udi** | **rdi** | **audio** | **tones** | **video**}

no bearer-capability clear-channel

Syntax Description

speech	Specifies speech as the information transfer capability (default).
udi	Specifies untrestricted digital information (UDI).
rdi	Specifies restricted digital information (RDI).
audio	Specifies 3.1 kHz audio.
tones	Specifies UDI with tones and announcements.
video	Specifies video as the information transfer capability.

Command Default

The default information transfer capability setting for the bearer-capability IE is **speech**.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

When a Cisco voice gateway receives a SIP early-media call and negotiates the clear-channel codec, the default for the information transfer capability octet (octet 3) of the bearer capability IE in the outgoing ISDN SETUP message is set to **speech**. Use the **bearer-capability clear-channel** command to change the information transfer capability of the bearer capability IE to a different value.

Note Changing the information transfer capability of the bearer capability IE affects only SIP early-media calls. The information transfer capability value is always **speech** for SIP delayed-media calls, even when the clear-channel codec is negotiated.

You can display the current information transfer capability setting for the bearer capability IE using the **show running-config** command. To show only voice service configuration information, limit the display output to the section on voice service (see the "Examples" section).

Note When the information transfer capability is set to the default value (**speech**), the output of the **show running-config** command does not include the bearer-capability information line.

Examples

The following examples show how to configure the information transfer capability of the bearer capability IE to UDI to allow for 64 kb/s data transfer over ISDN and how to display the current setting.

Use the following commands to change the information transfer capability setting in the bearer capability IE to **udi**:

```
voice service voip
 sip
  bearer-capability clear-channel udi
```

Use the following command to display the current information transfer capability setting:

```
Router# show running-config | section voice service

voice service voip
 h323
 sip
  bearer-capability clear-channel udi
```

billing b-channel

To enable the H.323 gateway to access B-channel information for all H.323 calls, use the **billing b-channel** command in H.323 voice service configuration mode. To return to the default setting, use the **no** form of this command.

billing b-channel

no billing b-channel

Syntax Description

This command has no arguments or keywords.

Command Default

B-channel information is disabled.

Command Modes

H.323 voice service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command enables the H.323 application to receive B-channel information of incoming ISDN calls. The B-channel information appears in H.323 ARQ / LRQ messages and can be used during call transfer or to route a call.

Examples

The following example adds B-channel information to the H.323 gateway:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# billing b-channel
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

bind

To bind the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface, use the **bind** command in SIP configuration mode. To disable binding, use the **no** form of this command.

bind {**control** | **media** | **all**} **source-interface** *interface-id* [**ipv4-address** *ipv4-address* | **ipv6-address** *ipv6-address*]

no bind

Syntax Description

control	Binds Session Initiation Protocol (SIP) signaling packets.
media	Binds only media packets.
all	Binds SIP signaling and media packets. The source address (the address that shows where the SIP request came from) of the signaling and media packets is set to the IPv4 or IPv6 address of the specified interface.
source-interface	Specifies an interface as the source address of SIP packets.
interface-id	Specifies one of the following interfaces: • **Async**: ATM interface • **BVI**: Bridge-Group Virtual Interface • **CTunnel**: CTunnel interface • **Dialer**: Dialer interface • **Ethernet**: IEEE 802.3 • **FastEthernet**: Fast Ethernet • **Lex**: Lex interface • **Loopback**: Loopback interface • **Multilink**: Multilink-group interface • **Null**: Null interface • **Serial**: Serial interface (Frame Relay) • **Tunnel**: Tunnel interface • **Vif**: PGM Multicast Host interface • **Virtual-Template**: Virtual template interface • **Virtual-TokenRing**: Virtual token ring
ipv4-address *ipv4-address*	(Optional) Configures the IPv4 address. Several IPv4 addresses can be configured under one interface.
ipv6-address *ipv6-address*	(Optional) Configures the IPv6 address under an IPv4 interface. Several IPv6 addresses can be configured under one IPv4 interface.

Command Default

Binding is disabled.

Command Modes SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 in this release.
12.3(4)T	The **media** keyword was added.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5

Usage Guidelines Async, Ethernet, FastEthernet, Loopback, and Serial (including Frame Relay) are interfaces within the SIP application.

If the **bind** command is not enabled, the IPv4 layer still provides the best local address.

Examples The following example sets up binding on a SIP network:

```
Router(config)# voice serv voip
Router(config-voi-serv)# sip
Router(config-serv-sip)# bind control source-interface FastEthernet 0
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice service VoIP configuration mode.

bind interface

To bind an interface to a Cisco CallManager group, use the **bind interface** command in SCCP Cisco CallManager configuration mode. To unbind the selected interface, use the **no** form of this command.

bind interface {**dynamic** | *interface-type interface-number*}

no bind interface {**dynamic** | *interface-type interface-number*}

Syntax Description

dynamic	The transcoder interface is chosen based on the remote IP address.
interface-type	Type of selected interface.
interface-number	Number of the selected interface.

Command Default

Interfaces are not associated with any Cisco CallManager group.

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.1(3)T1	This command was modified. The **dynamic** keyword was added.

Usage Guidelines

Normally a firewall only opens certain addresses or port combination to the outside world and those addresses can change dynamically. The VoIP technology requires the use of more than one address or port combination to pass information. The **bind interface** command allows administrators to dictate the use of one network to transport the signaling and another network to transport the media by assigning an interface to a Cisco CallManager group for a specific interface for the signaling or media application.

The selected interface is used for all calls that belong to the profiles that are associated to this Cisco CallManager group. If the **dynamic** keyword is configured, the transcoder interface is chosen based on the remote address. If the interface is not configured, the Skinny Call Control Protocol (SCCP) selects the best interface IP address in the gateway. Interfaces are selected according to user requirements. If there is only one group interface, configuration is not needed.

Note Only one interface can be selected. A given interface can be bound to more than one Cisco CallManager group.

Examples

The following example binds the interface to a specific Cisco CallManager group:

```
Router(config-sccp-ccm)# bind interface fastethernet 2:1
```

Related Commands

Command	Description
associate profile	Associates a DSP farm profile with a Cisco CallManager group.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.

block

To configure global settings to drop (not pass) specific incoming Session Initiation Protocol (SIP) provisional response messages on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE), use the **block** command in voice service SIP configuration mode. To disable a global configuration to drop incoming SIP provisional response messages, use the **no** form of this command.

block {**180** | **181** | **183**} [**sdp** {**absent** | **present**}]

no block {**180** | **181** | **183**}

Syntax Description

180	Specifies that incoming SIP 180 Ringing messages should be dropped (not passed to the other leg).
181	Specifies that incoming SIP 181 Call is Being Forwarded messages should be dropped (not passed to the other leg).
183	Specifies that incoming SIP 183 Session in Progress messages should be dropped (not passed to the other leg).
sdp	(Optional) Specifies that either the presence or absence of Session Description Protocol (SDP) information in the received response determines when the dropping of specified incoming SIP messages takes place.
absent	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is absent from the received provisional response.
present	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is present in the received provisional response.

Command Default

Incoming SIP 180, 181, and 183 provisional responses are forwarded.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced. Only SIP 180 and SIP 183 messages are supported on Cisco UBEs.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. Support was added for SIP 181 messages on the Cisco IOS SIP gateway, SIP-SIP Cisco UBEs, and the SIP trunk of Cisco Unified Communications Manager Express (Cisco Unified CME).
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **block** command in voice service SIP configuration mode to globally configure Cisco IOS voice gateways and Cisco UBEs to drop specified SIP provisional response messages. Additionally, you can use the **sdp** keyword to further control when the specified SIP message is dropped based on either the absence or presence of SDP information.

To configure settings for an individual dial peer, use the **voice-class sip block** command in dial peer voice configuration mode. To disable global configurations for dropping specified incoming SIP messages on a Cisco IOS voice gateway or Cisco UBE, use the **no block** command in voice service SIP configuration mode.

Note This command is supported only on outbound dial peers—it is nonoperational if configured on inbound dial peers. You should configure this command on the outbound SIP leg that sends out the initial INVITE message. Additionally, this feature applies only to SIP-to-SIP calls and will have no effect on H.323-to-SIP calls.

Examples

The following example shows how to globally configure dropping of incoming SIP provisional response messages:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# block 181
```

The following example shows how to globally configure dropping of incoming SIP with SDP provisional response messages:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# block 183 sdp present
```

The following example shows how to globally configure dropping of incoming SIP without SDP provisional response messages:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# block 180 sdp absent
```

The following example shows how to globally configure passing all specified incoming SIP provisional response messages (except for those on individual dial peers that are configured to override the global configuration):

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# no block 181
```

Related Commands

Command	Description
map resp-code	Configures global settings on a Cisco UBE for mapping specific incoming SIP provisional response messages to a different SIP response message.
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or Cisco UBE to drop specified SIP provisional response messages.
voice-class sip map resp-code	Configures a specific dial peer on a Cisco UBE to map specific incoming SIP provisional response messages to a different SIP response message.

block-caller

To configure call blocking on caller ID, use the **block-caller** command in dial peer voice configuration mode. To disable call blocking on caller ID, use the **no** form of this command.

block-caller *number*

no block-caller *number*

Syntax Description

number	Specifies the telephone number to block. You can use a period (.) as a digit wildcard. For example, the command **block-caller 5.51234** blocks all numbers beginning with the digit 5, followed by any digit, and then sequentially followed by the digits 5, 1, 2, 3, and 4.

Command Default

Call blocking is disabled; the router does not block any calls for any listed directory numbers (LDNs) based on caller ID numbers

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.1(2)XF	This command was introduced on the Cisco 800 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

This command is available on Cisco 800 series routers that have plain old telephone service (POTS) ports. For each dial peer, you can enter up to ten caller ID numbers to block. The routers do not accept additional caller ID numbers if ten numbers are already present. In that case, a number must be removed before another caller ID number can be added for blocking.

If you do not specify the **block-caller** command for a local directory, all voice calls to that local directory are accepted. If you specify the **block-caller** command for a local directory, the router verifies that the incoming calling-party number does not match any caller ID numbers in that local directory before processing or accepting the voice call. Each specified caller ID number and incoming calling-party number is compared from right to left, up to the number of digits in the specified caller ID number or incoming calling-party number, whichever has fewer digits.

This command is effective only if you subscribe to caller ID service. If you enable call blocking on caller ID without subscribing to the caller ID service, the routers do not perform the verification process on calling-party numbers and do not block any calls.

Examples

The following example configures a router to block calls from a caller whose caller ID number is 408-555-0134.

```
dial-peer voice 1 pots
 block-caller 4085550134
```

Related Commands

Command	Description
caller-id	Identifies incoming calls with caller ID.
debug pots csm csm	Activates events from which an application can determine and display the status and progress of calls to and from POTS ports.
isdn i-number	Configures several terminal devices to use one subscriber line.
pots call-waiting	Enables local call waiting on a router.
registered-caller ring	Configures the Nariwake service registered caller ring cadence.

bootup e-lead off

To prevent an analog ear and mouth (E&M) voice port from keying the attached radio on router boot up, use the **bootup e-lead off** command in voice-port configuration mode. To allow the analog E&M voice port to key the attached radio on boot up, use the **no** form of this command.

bootup e-lead off

no bootup e-lead off

Syntax Description

This command has no arguments or keywords.

Command Default

The analog E&M voice port keys the attached radio on radio boot up.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command configures the E-lead behavior on boot up for both voice ports on the voice interface card (VIC).

Examples

The following example configures the analog E&M voice port to not key the attached radio on router boot up:

```
voice-port 1/0/0
 bootup e-lead off
```

busyout forced

To force a voice port into the busyout state, use the **busyout forced** command in voice-port configuration mode. To remove the voice port from the busyout state, use the **no** form of this command.

busyout forced

no busyout forced

Syntax Description

This command has no arguments or keywords.

Command Default

The voice-port is not in the busyout state.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600s series and Cisco 3600 series. On the Cisco MC3810, the **voice-port busyout** command was eliminated in favor of this command.
12.1(2)T	The command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

If a voice port is in the forced busyout state, only the **no busyout forced** command can restore the voice port to service.

To avoid conflicting command-line interface (CLI) commands, do not use the **busyout forced** command and the **ds0 busyout** command on the same controller.

Examples

The following example forces analog voice port 3/1/1 on a Cisco 3600 router into the busyout state:

```
voice-port 3/1/1
 busyout forced
```

The following example forces digital voice port 0/0:12 on a Cisco 3600 router into the busyout state:

```
voice-port 0/0:12
 busyout forced
```

Related Commands

Command	Description
busyout-monitor interface	Configures a voice port to monitor a serial interface for events that would trigger a voice-port busyout.
busyout seize	Changes the busyout seize procedure for a voice port.
show voice busyout	Displays information about the voice busyout state.

busyout monitor

To place a voice port into the busyout monitor state, enter the **busyout monitor** command in voice-port configuration mode. To remove the busyout monitor state from the voice port, use the **no** form of this command.

busyout monitor {**serial** *interface-number* | **ethernet** *interface-number* | **keepalive**} [**in-service**]

no busyout monitor {**serial** *interface-number* | **ethernet** *interface-number* | **keepalive**}

Syntax Description

serial	Specifies monitoring of a serial interface. More than one interface can be entered for a voice port.
ethernet	Specifies monitoring of an Ethernet interface. More than one interface can be entered for a voice port.
interface-number	The interface to be monitored for the voice port busyout function.
keepalive	In case of keepalive failures, the selected voice port or ports is busied out.
in-service	(Optional) Configures the voice port to be busied out when any monitored interface comes into service (its state changes to up). If the keyword is not entered, the voice port is busied out when all monitored interfaces go out of service (their state changes to down).

Command Default

The voice port does not monitor any interfaces.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.
12.0(5)XE	This command was implemented on the Cisco 7200 series.
12.0(5)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series and integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	The ability to monitor an Ethernet port was introduced and the **in-service** keyword was added. The **serial** keyword was first supported on the Cisco 2600 series and Cisco 3600 series.
12.1(1)T	The implementation of this command on the Cisco 7200 series was integrated into Cisco IOS Release 12.1(1)T.
12.1(2)T	The **serial** and **ethernet** keywords were added, the **in-service** keyword was integrated into Cisco IOS Release 12.1(2)T, and the *interface-number* argument was added to the **serial** and **ethernet** keywords.
12.1(3)T	The **interface** keyword was removed.
12.4(6)T	The **keepalive** keyword was added.

Usage Guidelines

When you place a voice port in the busyout monitor state, the voice port monitors the specified interface and enters the busyout state when the interface is down. This down state forces the rerouting of calls.

The **busyout monitor** command monitors only the up or down status of an interface—not end-to-end TCP/IP connectivity.

When an interface is operational, a busied-out voice port returns to its normal state.

This feature can monitor LAN, WAN, and virtual subinterfaces.

A voice port can monitor multiple interfaces at the same time. To configure a voice port to monitor multiple interfaces, reenter the **busyout monitor** command for each additional interface to be monitored.

If you specify more than one monitored interface for a voice port, all the monitored interfaces must be down to trigger busyout on the voice port.

You can combine in-service and out-of-service monitoring on a voice port. The following rule describes the action if monitored interfaces change state. A voice port is busied out if either of the following occurs:

- Any interface monitored for coming into service comes up.
- All interfaces monitored for going out of service go down.

Examples

The following example shows configuration of analog voice port 1/2 to busy out if serial port 0 or 1 comes into service:

```
voice-port 1/2
 busyout monitor serial 0 in-service
 busyout monitor serial 1 in-service
```

The following example shows configuration of digital voice port 1/2/2 on a Cisco 3600 series router to busy out if serial port 0 goes out of service:

```
voice-port 1/2/2
 busyout monitor serial 0
```

The following example shows configuration of the voice port to monitor two serial interfaces and an Ethernet interface. When all these interfaces are down, the voice port is busied out. When at least one interface is operating, the voice port is put back into a normal state.

```
voice-port 3/0:0
 busyout monitor ethernet 0/0
 busyout monitor serial 1/0
 busyout monitor serial 2/0
```

The following example shows configuration of the voice port to be busied out in case of a keepalive failure:

```
voice-port 10
 busyout monitor keepalive
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor probe	Configures a voice port to enter busyout state if an SAA probe signal returned from a remote interface crosses a delay or loss threshold.

busyout seize	Changes the busyout seize procedure for a voice port.
show voice busyout	Displays information about the voice busyout state.
voice-port busyout	Places all voice ports associated with a serial or ATM interface into a busyout state.

busyout monitor action

To place a voice port into graceful or shutdown busyout state when triggered by the busyout monitor, use the **busyout monitor action** command in voice-port configuration mode. To remove the voice port from the busyout state, use the **no** form of this command.

busyout monitor action {**graceful** | **shutdown** | **alarm blue**}

no busyout monitor action {**graceful** | **shutdown** | **alarm blue**}

Syntax Description

graceful	Graceful busyout state.
shutdown	D-channel shutdown busyout state.
alarm blue	Shutdown state with a blue alarm, also known as an alarm-indication signal (AIS).

Command Default

Default voice busyout behavior without this command is a forced busyout.

Default voice busyout behavior for PRI depends on whether or not the ISDN switch type supports service messages:

- If the switch type supports service messages, default voice busyout behavior is to transmit B-channel out-of-service (OOS) messages and to keep the D channel active. D-Channel service-messages are supported on the following ISDN switch-types: NI, 4ESS (User Side only), 5ESS (User Side only), DMS100.
- If the switch type does not support service messages, default voice busyout behavior is to bring down the D channel.
- For switch-types not specified above, the D-channel is taken down when the **busyout monitor action graceful** is configured.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(13)T	The **busyout monitor action graceful** command was introduced on the following platforms: Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3640, Cisco 3660, Cisco 3725, and Cisco VG200.
12.3(6)	The **busyout monitor action shutdown** command was introduced on the following platforms: Cisco 1700 series, Cisco IAD2420 series, Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3600 series, Cisco 3700 series, Cisco 4224, Cisco 7200 series, Cisco 7301, Cisco 7400 series, Cisco MC3810, Cisco WS-X4604-GWY, and Cisco VG200.
12.3(7)T	The **busyout monitor action shutdown** command was integrated into Cisco IOS Release 12.3(7)T and support was added for the Cisco IAD2430 series.

Release	Modification
12.4(6)T	The **busyout monitor action graceful** and **busyout monitor action shutdown** commands were introduced to replace the **busyout action graceful** and **busyout action shutdown** commands.
12.4(9)T	The **busyout monitor action** command was introduced to combine the **busyout monitor action graceful** and **busyout monitor action shutdown** commands. The **shutdown alarm blue** keywords were added.

Usage Guidelines

Use this command to control busyout behavior that is triggered by the **busyout monitor** command.

This command with the **graceful** keyword busies out the voice port immediately or, if there is an active call on this voice port, waits until the call is over.

This command with the **shutdown** keyword has the following attributes:

- Before Cisco IOS Release 12.2(8)T, when voice busyout is triggered on a PRI voice port, the D channel is deactivated until the busyout trigger is cleared. Some ISDN switch types, however, support in-service and OOS Q.931 messages that permit B channels to be taken out of service while still keeping the D channel active. Starting in Cisco IOS Release 12.3(8)T for these ISDN switch types, OOS messages are sent and the D channel is kept active when a voice busyout is triggered.
- This keyword is available only for PRI voice ports.
- For switch-types not specified above, the D-channel is be taken down when the **busyout monitor action graceful** command is configured.

Examples

The following example shows analog voice-port busyout state set to graceful:

```
voice-port 2/0:15
 busyout monitor action graceful
```

The following example shows E1 PRI voice-port busyout state set to shutdown:

```
voice-port 1/1:15 (E1 PRI)
 busyout monitor gatekeeper
 busyout monitor action shutdown
```

The following example shows T1 PRI voice-port busyout state set to shutdown:

```
voice-port 0/1:23 (T1 PRI)
 busyout monitor gatekeeper
 busyout monitor action shutdown
```

Related Commands

Command	Description
busyout forced	Forces a voice port into busyout state.
busyout monitor	Configures a voice port to monitor an interface for events that would trigger voice-port busyout.
busyout monitor backhaul	Configures a voice port to enter busyout-monitor state with backhaul-L3 connectivity monitoring during a WAN failure.
busyout monitor gatekeeper	Configures a voice port to enter busyout state if connectivity to the gatekeeper is lost.

Command	Description
busyout monitor probe	Configures a voice port to enter busyout state if an SAA probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
busyout seize	Changes the busyout seize procedure for a voice port.
show voice busyout	Displays information about voice-busyout state.
voice-port	Enters voice-port configuration mode and identifies the voice port to be configured.

busyout monitor backhaul

To configure a voice port to enter busyout-monitor state with backhaul-L3 connectivity monitoring during a wide-area-network (WAN) failure, use the **busyout monitor backhaul** command in voice-port configuration mode. To disable busyout-monitor state, use the **no** form of this command.

busyout monitor backhaul

no busyout monitor backhaul

Syntax Description This command has no arguments or keywords.

Command Default If this command is not used, the voice port is not configured to enter busyout state during a WAN failure.

Command Modes Voice-port configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines Use this command to implement backhaul-L3 connectivity monitoring.

Examples The following example configures a voice port to enter busyout-monitor state with backhaul-L3 connectivity monitoring during a WAN failure:

```
Router(config-voiceport)# busyout monitor backhaul
```

Related Commands

Command	Description
busyout monitor action	Places a voice port into busyout state.
busyout monitor	Configures a voice port to enter busyout-monitor state.

busyout monitor gatekeeper

To configure a voice port to enter the busyout state if connectivity to the gatekeeper is lost, use the **busyout monitor gatekeeper** command in voice-port configuration mode. To configure the monitor to trigger a busyout when any voice port assigned to a specific voice class loses connectivity to the gatekeeper, use the **busyout monitor gatekeeper** command in voice-class configuration mode. To disable the busyout monitoring state for the gatekeeper, use the **no** form of this command.

busyout monitor gatekeeper

no busyout monitor gatekeeper

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not used, the voice port or voice class is not configured to enter a busyout state if connectivity to the gatekeeper is lost.

Command Modes

Voice-port configuration
Voice-class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3640, Cisco 3660, Cisco 3725 and Cisco VG200.
12.4(6)T	This command was extended to include functionality in voice-class configuration mode.

Usage Guidelines

Use this command to monitor the connection between the gateway and gatekeeper.

Examples

The following example shows the busyout monitor state set to busyout the port according to the state of the gatekeeper:

```
voice-port 1/1/1
 busyout monitor gatekeeper
```

The following example enters voice-class (busyout) configuration mode and creates a voice class named 33. The monitor is set to busyout when any voice port in voice class 33 loses connectivity to the gatekeeper:

```
voice-class busyout 33
 busyout monitor gatekeeper
```

Related Commands

Command	Description
busyout monitor action graceful	Places a voice port into the graceful busyout state when triggered by the busyout monitor.
busyout monitor action graceful	Shuts down the voice port immediately, but if there is an active call it waits until the call is over.
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Configures a voice port to monitor an interface for events that would trigger a voice-port busyout.
busyout monitor probe	Configures a voice port to enter the busyout state if an SAA probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
busyout seize	Changes the busyout seize procedure for a voice port.
show voice busyout	Displays information about the voice busyout state.
voice-port	Enters voice-port configuration mode and identifies the voice port to be configured.

busyout monitor probe

To configure a voice port to enter the busyout state if a Service Assurance Agent (SAA) probe signal is returned from a remote IP-addressable interface after the expiration of a specified delay or loss threshold, use the **busyout monitor probe** command in voice-port configuration mode or voice class busyout mode. To configure a voice port not to monitor SAA probe signals, use the **no** form of this command.

busyout monitor probe [**icmp-ping**] *ip-address* [**codec** *codec-type* | **size** *bytes*] [**icpif** *number* | **loss** *percent* **delay** *milliseconds*] [**grace-period** *seconds*] size

no busyout monitor probe *ip-address*

Syntax Description

icmp-ping	(Optional) Configures voice-port parameters to use ICMP pings to monitor IP destinations.
ip-address	The IP address of a target interface for the SAA probe signal.
codec	(Optional) Configures the profile of the SAA probe signal to mimic the packet size and interval of a specific codec type.
codec-type	(Optional) The codec type for the SAA probe signal. Available options are as follows: • **g711a**—G.711 a-law • **g711u**—G.711 mu-law (the default) • **g729**—G.729 • **g729a**—G.729 Annex A • **g729b**—G.729 Annex B
size *bytes*	(Optional) Size (in bytes) of the ping packet. Default is 32.
icpif	(Optional) Configures the busyout monitor probe to use an Impairment/Calculated Planning Impairment Factor (ICPIF) loss/delay busyout threshold, in accordance with ITU-T G.113. The ICPIF numbers represent predefined combinations of loss and delay.
number	(Optional) The ICPIF threshold for initiating a busyout condition. Range is from 0 to 30. Low numbers are equivalent to low loss and delay thresholds.
loss	(Optional) Configures the percentage-of-packets-lost threshold for initiating a busyout condition.
percent	(Optional) The loss value (expressed as a percentage) for initiating a busyout condition. Range is from 1 to 100.
delay	(Optional) Configures the average packet delay threshold for initiating a busyout condition.
milliseconds	(Optional) The delay threshold, in milliseconds, for initiating a busyout condition. Range is from 1 to 2,147,483,647.
grace-period	(Optional) Configures a time limit that the system waits before initiating a busyout condition after the loss of SAA probe connectivity.
seconds	(Optional) Number of seconds for the duration of the grace period. Range is from 30 to 300.

Command Default

If the **busyout monitor probe** command is not entered, the voice port does not monitor SAA probe signals.

If the **busyout monitor probe** command is entered with no optional keywords or arguments, the default codec type is G.711 a-law, the default loss and delay thresholds are the threshold values that are configured with the **call fallback threshold delay-loss** command, and the loss of SAA connectivity causes an immediate forced busyout condition.

Command Modes

Voice-port configuration and voice class busyout

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 and Cisco 3600 series and on the Cisco MC3810.
12.3(15)	This command was integrated into Cisco IOS Release 12.3(15) and the **grace-period** keyword and *seconds* argument were added.
12.4(1)	This command was integrated into Cisco IOS Release 12.4(1).
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

A voice port can monitor multiple interfaces at the same time. To configure a voice port to monitor multiple interfaces, enter the **busyout monitor probe** command for each additional interface to be monitored.

Caution The **busyout monitor probe** command is effective only if the call fallback function is enabled on the source router, and the SAA responder is enabled on the target router. To enable the call fallback function, you must enter the **call fallback active** command for the **busyout monitor probe** command to work.

The SAA probe is transmitted periodically with a period determined by the call fallback function.

Low thresholds of ICPIF, loss, and delay result in early busyout when the link deteriorates, thereby raising the voice minimum quality level. High thresholds prevent busyout until loss and delay are long, allowing transmission of lower-quality voice.

Caution If thresholds are set too low, the link can alternate between in-service and out-of-service states, causing repeated interruptions of traffic.

Before the introduction of the **grace-period** keyword to the **busyout monitor probe** command, the loss of SAA probe connectivity was sufficient to immediately enforce busyout, causing service and connectivity problems in some networks because busyout conditions could occur frequently and abruptly. To improve busyout monitoring via SAA probes, the **grace-period** setting allows for an additional timer that must expire before a busyout condition is enforced. That is, the SAA probes and the period of grace must both expire before a busyout condition is invoked. If the SAA IP connectivity is restored within the period of grace, the busyout condition does not occur.

Note To disable the **grace-period** option, you must first enter the **no busyout monitor probe** command and then re-enter the **busyout monitor probe** command without the **grace-period** option.

The **grace-period** keyword is not available in Cisco IOS Release 12.3T.

Examples

The following example shows how to configure analog voice port 1/1/0 to use an SAA probe with a G.711a-law profile to probe the link to two remote interfaces that have IP addresses and to busy out the voice port if SAA probe connectivity is lost for at least 5 seconds. Both links have a loss exceeding 25 percent or a packet delay of more than 1.5 seconds.

```
voice-port 1/1/0
 busyout monitor probe 209.165.202.128 codec g711a loss 25 delay 1500 grace-period 45
 busyout monitor probe 209.165.202.129 codec g711a loss 25 delay 1500 grace-period 45
```

Related Commands

Command	Description
busyout monitor	Places a voice port into the busyout monitor state.
call fallback active	Enables the ICMP-ping or SAA (formerly RTR) probe mechanism for use with the dial-peer **monitor probe** or voice-port **busyout monitor probe** commands.
call fallback threshold delay-loss	Forces a voice port into the busyout state.
show voice busyout	Displays information about the voice busyout state.
voice class busyout	Creates a voice class for local voice busyout functions.

busyout seize

To change the busyout action for a Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **busyout seize** command in voice-port configuration mode. To restore the default busyout action, use the **no** form of this command.

busyout seize {**ignore** | **repeat**}

no busyout seize

Syntax Description

ignore	Specifies the type of ignore procedure, depending on the type of voice port signaling. See Table 1 for more information.
repeat	Specifies the type of repeat procedure, depending on the type of voice port signaling. See Table 1 for more information.

Command Default

See Table 1 for the default actions for different voice ports and signaling types

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **busyout seize** command is valid for both analog and digital voice ports. On digital voice ports, the busyout actions are valid whether the busyout results from a voice-port busyout event or from the **ds0-busyout** command.

The voice port returns to an idle state when the event that triggered the busyout disappears.

Table 1 describes the busyout actions for the **busyout seize** settings on each voice port type.

The busyout action for E and M voice ports is to seize the far end by setting lead busy.

Table 1 Busyout Seize Actions for Voice Ports

Voice Port Signaling Type	Procedure Setting (busyout-option command)	Busyout Actions
FXS loop start	Default	Removes the power from the loop. For analog voice ports, this is equivalent to removing the ground from the tip lead. For digital voice ports, the port generates the bit pattern equivalent to removing the ground from the tip lead, or it busies out if the bit pattern exists.
FXS loop start	Ignore	Ignores the ground on the ring lead.
FXS ground start	Default	Grounds the tip lead and stays at this state.
FXS ground start	Ignore	1. Leaves the tip lead open. 2. Ignores the ground on the ring lead.
FXS ground start	Repeat	1. Grounds the tip lead. 2. Waits for the far end to close the loop. 3. The far end closes the loop. 4. If the far end then opens the loop, FXS removes the ground from the tip lead. 5. FXS waits for several seconds before returning to Step 1.
FXO loop start	Default	Closes the loop and stays at this state.
FXO loop start	Ignore	1. Leaves the loop open. 2. Ignores the ringing current on the ring level.
FXO loop start	Repeat	1. Closes the loop. 2. After the detected far end starts the power denial procedure, FXO opens the loop. 3. After the detected far end has completed the power denial procedure, FXO waits for several seconds before returning to Step 1.
FXO ground start	Default	Grounds the tip lead.
FXO ground start	Ignore	1. Leaves the loop open. 2. Ignores the running current on the ring lead, or the ground current on the tip lead.
FXO ground start	Repeat	1. Grounds the ring lead. 2. Removes the ground from the ring lead and closes the loop after the detected far end grounds the tip lead. 3. When the detected far end removes the ground from tip lead, FXO opens the loop. 4. FXO waits for several seconds before returning to Step 1.

Examples

The following example shows configuration of analog voice port 1/1 to perform the ignore actions when busied out:

```
voice-port 1/1
 busyout seize ignore
```

The following example shows configuration of digital voice port 0:2 to perform the repeat actions when busied out:

```
voice-port 0:2
 busyout seize repeat
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout-monitor interface	Configures a voice port to monitor an interface for events that would trigger a voice port busyout.
ds0 busyout	Forces a DS0 time slot on a controller into the busyout state.
show voice busyout	Displays information about the voice busyout state.
voice-port busyout	Places all voice ports associated with a serial or ATM interface into a busyout state.

Cisco IOS Voice Commands: C

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

cac master

To configure the call admission control (CAC) operation as master, enter the **cac master** command in voice-service configuration mode. To restore CAC operation to slave, use the **no** form of this command.

cac master

no cac master

Syntax Description

This command has no arguments or keywords.

Defaults

CAC operation is slave

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

You should configure the router at opposite ends of an ATM adaptation layer 2 (AAL2) trunk for the opposite CAC operation—master at one end and slave at the other end.

A router configured as a master always performs CAC during fax and modem upspeed. A router configured as a slave sends a request for CAC to the CAC master.

Examples

The following example shows configuration of the CAC operation of a router as master:

```
voice service voatm
 session protocol aal2
 cac master
```

The following example shows configuration of these entities being returned to slave status:

```
voice service voatm
 session protocol aal2
 no cac master
```

cac_off

To disable connection admission control (CAC), use the **cac_off** command in interface-ATM-VC configuration mode. To enable CAC, use the **no** form of this command.

cac_off

no cac_off

Syntax Description This command has no keywords or arguments.

Command Default Call admission control is enabled.

Command Modes Interface-ATM-VC configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines Connection admission control (CAC) is a set of actions taken by each ATM switch during connection setup to determine whether the requested quality of service (QoS) will violate the QoS guarantees for established connections. CAC reserves bandwidth for voice calls, however, the bandwidth required when the lossless compression codec (LLCC) is used is dynamic and usually less than what is generally reserved by CAC. Disabling CAC can help in better utilization of bandwidth when LLCC is used.

Examples The following example disables call admission control on a PVC:

```
interface ATM0/IMA1.1 point-to-point
 pvc test1 15/135
  cac_off
```

cache (neighbor BE)

To configure the local border element (BE) to cache the descriptors received from its neighbors, use the **cache** command in neighbor BE configuration mode. To disable caching, use the **no** form of this command.

cache

no cache

Syntax Description

This command has no arguments or keywords.

Defaults

Caching is not enabled

Command Modes

Neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to configure the local BE to cache the descriptors received from its neighbor. If caching is enabled, the neighbors are queried at the specified interval for their descriptors.

Examples

The following example shows the border element enabled to cache the descriptors from its neighbors.

```
Router(config-annexg-neigh)# id neighbor-id
Router(config-annexg-neigh)# cache
```

Related Commands

Command	Description
id	Configures the local ID of the neighboring BE.
port	Configures the neighbor's port number that is used for exchanging Annex G messages.
query-interval	Configures the interval at which the local BE queries the neighboring BE.

cache reload time (global application configuration mode)

To configure the router to reload scripts from cache on a regular interval, use the **cache reload time** command in global application configuration mode. To set the value to the default, use the **no** form of this command.

cache reload time *bg-minutes*

no cache reload time

Syntax Description

bg-minutes	Number of minutes after which the background process is awakened. This background process checks the time elapsed since the script was last used and whether the script is current: • If the script has not been used in the last "unload time," it unloads the script and quits. The unload time is not configurable. • If the script has been used, the background process loads the script from the URL. It compares the scripts, and if they do not match, it begins using the new script for new calls.

Command Default 30 minutes

Command Modes Global application configuration

Command History

Release	Modification
12.3(14)T	The **call application cache reload time** command was moved to global application configuration mode and changed to **cache reload time**.

Examples The following example displays the **cache reload time** command configured to specify 15 minutes before a background process is awakened:

Enter application configuration mode to configure applications and services:

```
application
```

Enter global application configuration mode:

```
global
```

Configure the cache reload time:

```
cache reload time 15
```

Related Commands

Command	Description
call application cache reload time	Configures the router to reload the MGCP scripts from cache on a regular interval.
show call application voice	Displays all Tcl or MGCP scripts that are loaded.

cadence

To define the tone-on and tone-off durations for a call-progress tone, use the **cadence** command in call-progress dualtone configuration mode. To restore the default cadence, use the **no** form of this command.

cadence {*cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time*] [*cycle-3-on-time cycle-3-off-time*] [*cycle-4-on-time cycle-4-off-time*]} | **continuous**

no cadence

Syntax Description

cycle-1-on-time	Tone-on duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.
cycle-1-off-time	Tone-off duration for the first cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-2-on-time	(Optional) Tone-on duration for the second cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-2-off-time	(Optional) Tone-off duration for the second cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-3-on-time	(Optional) Tone-on duration for the third cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-3-off-time	(Optional) Tone-off duration for the third cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-4-on-time	(Optional) Tone-on duration for the fourth cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
cycle-4-off-time	(Optional) Tone-off duration for the fourth cycle of the cadence pattern, in milliseconds. Range is from 0 to 1000. The default is 0.
continuous	Continuous call-progress tone is detected.

Command Default Continuous

Command Modes Call-progress dualtone configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750 and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command specifies the cadence for a class of custom call-progress tones.

You must define each cadence that you want a voice port to detect. Reenter the command for each additional cadence to be detected.

You must associate the class of custom call-progress tones with a voice port for this command to affect tone detection.

Examples

The following example defines a cadence for a busy tone in the custom-cptone voice class with the name "country-x." This example defines 500 ms tone on and 500 ms tone off.

```
voice class custom-cptone country-x
 dualtone busy
 cadence 500 500
```

The following example configures detection of the default frequency and cadence values for the busy tone in the custom-cptone voice class with the name "country-x". The default frequency is a 300 Hz tone, and the default cadence is continuous.

```
voice class custom-cptone country-x
 dualtone busy
 no cadence
 no frequency
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the boundaries and limits for custom call-progress tones defined by the **voice class custom-cptone** command.

cadence-list

To specify a tone cadence pattern to be detected, use the **cadence-list** command in voice-class configuration mode. To delete a cadence pattern, use the **no** form of this command.

cadence-list *cadence-id cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time*] [*cycle-3-on-time cycle-3-off-time*] [*cycle-4-on-time cycle-4-off-time*]

no cadence-list *cadence-id*

Syntax Description

cadence-id	A tag to identify this cadence list. The range is from 1 to 10.
cycle-1-on-time	The tone duration for the first cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-1-off-time	The silence duration for the first cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-2-on-time	(Optional) The tone duration for the second cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-2-off-time	(Optional) The silence duration for the second cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-3-on-time	(Optional) The tone duration for the third cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-3-off-time	(Optional) The silence duration for the third cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-4-on-time	(Optional) The tone duration for the fourth cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
cycle-4-off-time	(Optional) The silence duration for the fourth cycle of the cadence pattern. Range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.

Command Default

No cadence pattern is configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, the Cisco MC3810.

Usage Guidelines

A cadence list enables the router to match a complex tone pattern from a PBX or public switched telephone network (PSTN). A tone is detected if it matches any configured cadence list. You can create up to ten cadence lists, enabling the router to detect up to ten different tone patterns. If the tone to be detected consists of only one on-off cycle, you can configure this in either of two ways:

- Create a cadence list using only the *cycle-1-on-time* and *cycle-1-off-time variables*.
- Use the **cadence-max-off-time** and **cadence-min-on-time** commands.

You must also configure the times of the **cadence-max-off-time** and **cadence-min-on-time commands** to be compatible with the on and off times specified by the **cadence-list** command. The time of the **cadence-max-off-time** must be equal to or greater than the longest **off-time** in the cadence list; the **cadence-min-on-time** must be equal to or less than the shortest **on-time** in the cadence list.

Examples

The following example shows configuration of cadence list 1 with three on/off cycles and cadence list 2 with two on/off cycles for voice class 100:

```
voice class dualtone 100
 cadence-list 1 100 100 300 300 100 200
 cadence-list 2 100 200 100 400
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum *off* duration for detection of a tone.
cadence-min-on-time	Specifies the minimum *on* duration for detection of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

cadence-max-off-time

To specify the maximum time that a tone can be off and still detected as part of a cadence, use the **cadence-max-off-time** command in voice-class configuration mode. To restore the default, use the **no** form of this command.

cadence-max-off-time *time*

no cadence-max-off-time

Syntax Description

time	The maximum *off* time of a tone that can be detected, in 10-millisecond increments. Range is from 0 to 5000 (0 milliseconds to 50 seconds). The default is 0.

Command Default

0 (no off time)

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Specify a time value greater than the *off* time of the tone to be detected, and use a time value greater than 0 to enable detection of a cadenced tone. With the default (0), the router detects only a continuous tone.

Examples

The following example shows configuration of a maximum *off* duration of 20 seconds for voice class 100:

```
voice class dualtone 100
 cadence-max-off-time 2000
```

Related Commands

Command	Description
cadence-min-on-time	Specifies the minimum *on* duration for detection of a tone.
cadence-variation	Specifies the cadence variation time allowed for detection of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

cadence-min-on-time

To specify the minimum time that a tone can be on and still detected as part of a cadence, use the **cadence-min-on-time** command in voice-class configuration mode. To restore the default, use the **no** form of this command.

cadence-min-on-time *time*

no cadence-min-on-time

Syntax Description

time	The minimum *on* time of a tone that can be detected, in 10-millisecond increments. Range is from 0 to 100 (0 milliseconds to 1 seconds). The default is 0.

Command Default

0 (no minimum on time)

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Specify a time value shorter than the *on* time of the tone to be detected. With the default (0), a tone of any length is detected.

Examples

The following example shows configuration of a minimum *on* duration of 30 milliseconds (three 10-ms time intervals) for voice class 100:

```
voice class dualtone 100
 cadence-min-on-time 3
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum *off* duration for detection of a tone.
cadence-variation	Specifies the cadence variation time allowed for detection of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

cadence-variation

To specify the cadence variation time allowed for detection of a tone, use the **cadence-variation** command in voice-class configuration mode. To restore the default cadence variation time, use the no form of this command.

cadence-variation *time*

no cadence-variation

Syntax Description

time	The maximum time by which the tone onset can vary from the specified onset time and still be detected, in 10-millisecond increments. Range is from 0 to 200 (0 milliseconds to 2 seconds). The default is 0.

Command Default 0 milliseconds

Command Modes Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco MC3810.
12.1(5)XM	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750 router.

Usage Guidelines Specify a time value greater than the cadence variation of the tone to be detected. With the default of 0, only those tones that match the configured cadence are detected.

This command creates a detection limit for one parameter within a voice class. You can apply the detection limit to any voice port.

Examples The following example specifies a cadence variation time of 30 milliseconds for voice class 100:

```
voice class dualtone 100
 cadence-variation 3
```

The following example specifies 80 ms (eight 10-ms time intervals) as the maximum allowable cadence variation in voice class 70:

```
voice class dualtone-detect-params 70
 cadence-variation 8
```

Related Commands

Command	Description
cadence-max-off-time	Specifies the maximum *off* duration for detection of a tone.
cadence-min-on-time	Specifies the minimum *on* duration for detection of a tone.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters defined by the **voice class dualtone-detect-params** command to a voice port.

call accounting-template

To select an accounting template at a specific location, use the **call accounting-template** command in global configuration or application configuration mode. To deselect a specific accounting template, use the **no** form of this command.

call accounting-template *acctTempName url*

no call accounting-template *acctTempName url*

Syntax Description

acctTempName	Template name.
url	Location of the template.

Command Default

No default behavior or values

Command Modes

Global configuration
Application configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(14)T	This command was added to the application configuration mode to replace the **call application voice accounting-template** command.

Usage Guidelines

For call detail records, the template name must have a .cdr extension. To select call records based on your accounting needs and to specify the location of an accounting template that defines the applicable vendor-specific attributes (VSAs) for generating those selected call records, use the **call accounting-template** command in global configuration mode.

The *acctTempName* argument refers to a specific accounting template file that you want to send to the RADIUS server. This template file defines only specific VSAs selected by you to control your call records based on your accounting needs.

Examples

The example below shows the accounting template cdr1 selected from a specific TFTP address.

```
call accounting-template temp-ivr tftp://kyer/sample/cdr/cdr1.cdr
```

Related Commands

Command	Description
call application voice accounting-template	Configures T.37 fax accounting with VoIP AAA nonblocking API.
show call accounting-template voice	Selects an accounting template at a specific location.

call accounting-template voice

To select an accounting template at a specific location, use the **call accounting-template voice** command in global configuration mode. To remove a specific accounting template, use the **no** form of this command.

call accounting-template voice *acctTempName url*

no call accounting-template voice *acctTempName url*

Syntax Description

acctTempName	Template name.
url	Location of the template.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(14)T	The **call accounting-template voice** command is replaced by the **call accounting-template** command in application configuration mode. See the **call accounting-template** command for more information.

Usage Guidelines The template name must have a .cdr extension.

To select call records based on your accounting needs and to specify the location of an accounting template that defines the applicable vendor-specific attributes (VSAs) for generating those selected call records, use the **call accounting-template voice** command in global configuration mode.

The *acctTempName* argument refers to a specific accounting template file that you want to send to the RADIUS server. This template file defines only specific VSAs selected by you to control your call records based on your accounting needs.

Examples The example below shows the accounting template cdr1 selected from a specific TFTP address.

```
call accounting-template voice temp-ivr tftp://kyer/sample/cdr/cdr1.cdr
```

Related Commands

Command	Description
call accounting-template voice reload	Reloads the accounting template.
show call accounting-template voice	Selects an accounting template at a specific location.

call accounting-template voice reload

To reload the accounting template, use the **call accounting-template voice reload** command in privileged EXEC mode.

call accounting-template voice reload *acctTempName*

Syntax Description

reload	Reloads the accounting template from the address (for example, a tftp address) where the template is stored.
acctTempName	Name of the accounting template.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Use the **call accounting-template voice reload** command to reload the template from the URL defined in the **call accounting-template voice** command. After bootup, if the template file fails to load from the TFTP server, the system tries to automatically reload the file at 5-minute intervals.

Examples

The example below shows how to reload accounting template cdr2:

```
call accounting-template voice reload cdr2
```

Related Commands

Command	Description
call accounting-template voice	Selects an accounting template at a specific location
gw-accounting aaa	Defines and loads the template file at the location defined by the URL.
show call accounting-template voice	Displays the VSAs that are contained in the accounting template.

call-agent

To define the call agent for a Media Gateway Control Protocol (MGCP) profile, use the **call-agent** command in MGCP profile configuration mode. To return to the default values, use the **no** form of this command.

call-agent {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*]

no call-agent

Syntax Description

dns-name	Fully qualified domain name (including host portion) for the call agent. For example, “ca123.example.net”.
ip-address	IP address of the call agent.
port	(Optional) User Datagram Protocol (UDP) port number over which the gateway sends messages to the call agent. Range is from 1025 to 65535. • The default call-agent UDP port is 2727 for MGCP 1.0, Network-based Call Signaling (NCS) 1.0, and Trunking Gateway Control Protocol (TGCP) 1.0. • The default call-agent UDP port is 2427 for MGCP 0.1 and Simple Gateway Control Protocol (SGCP).
service-type *type*	(Optional) Protocol service type valid values for the *type* argument are **mgcp**, **ncs**, **sgcp**, and **tgcp**. The default service type is **mgcp**.
version *protocol-version*	(Optional) Version number of the protocol. Valid values follow: • Service-type MGCP—**0.1**, **1.0** • Service-type NCS—**1.0** • Service-type SGCP—**1.1**, **1.5** • Service-type TGCP—**1.0** The default service type and version are **mgcp** and **0.1**.

Command Default

The default call-agent UDP port is 2727 for MGCP 1.0, Network-based Call Signaling (NCS) 1.0, and Trunking Gateway Control Protocol (TGCP) 1.0.
The default call-agent UDP port is 2427 for MGCP 0.1 and Simple Gateway Control Protocol (SGCP).
The default service type and version are MGCP 0.1.

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when values for a MGCP profile are configured.

Call-agent configuration for an MGCP profile (with this command) and global call-agent configuration (with the **mgcp call-agent** command) are mutually exclusive; the first to be configured on an endpoint blocks configuration of the other on the same endpoint.

Identifying call agents by Domain Name System (DNS) name rather than by IP address in the **call-agent** command provides call-agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by a DNS name and a message from the gateway fails to reach the call agent, the **max1 lookup** and **max2 lookup** commands enable a search from the DNS lookup table for a backup call agent at a different IP address.

The *port* argument configures the call agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse, or the gateway port number (the UDP port over which the gateway receives messages from the call agent), is configured by specifying a port number in the **mgcp** command.

The service type **mgcp** supports the Restart In Progress (RSIP) error messages sent by the gateway if the **mgcp sgcp restart notify** command is enabled. The service type **sgcp** ignores the RSIP messages.

Examples

The following example defines a call agent for the MGCP profile named "tgcp_trunk":

```
Router(config)# mgcp profile tgcp_trunk
Router(config-mgcp-profile)# call-agent 10.13.93.3 2500 service-type tgcp version 1.0
```

Related Commands

Command	Description
max1 lookup	Enables DNS lookup of the MGCP call agent address when the suspicion threshold value is reached.
max2 lookup	Enables DNS lookup of the MGCP call agent address when the disconnect threshold value is reached.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp call-agent	Configures the address of the call agent (media gateway controller).
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

call application alternate

Note Effective with Cisco IOS Release 12.3(14)T, the **call application alternate** command is replaced by the **service** command in global application configuration mode. See the **service** command for more information.

To specify an alternate application to use if the application that is configured in the dial peer fails, use the **call application alternate** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

call application alternate [*application-name*]

no call application alternate

Syntax Description

application-name	(Optional) Name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Command Default The call is rejected if the application in the dial peer fails.

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(14)T	This command was replaced by the **service** command in global application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines If this command is not configured, calls are rejected when the dial peer that matches the call does not specify a valid voice application.

In releases before Cisco IOS Release 12.2(11)T, the default application (DEFAULT) was automatically triggered if no application was configured in the dial peer or if the configured application failed. The default application is no longer automatically executed unless the **call application alternate** command is configured.

The application named DEFAULT is a simple application that outputs dial tone, collects digits, and places a call to the dialed number. This application is included in Cisco IOS software; you do not have to download it or configure it by using the **call application voice** command.

The **call application alternate** command specifies that if the application that is configured in the dial peer fails, the default voice application is executed. If the name of a specific application is entered, that application is triggered if the application configured in the dial peer fails. If the alternate application also fails, the call is rejected.

If an application name is entered, that application must first be configured on the gateway by using the **call application voice** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application alternate

        Warning: This command has been deprecated. Please use the following:
                 service
```

The following example configures the DEFAULT application as the alternate:

```
call application alternate
```

The following example configures the application *session* as the alternate:

```
call application alternate session
```

Related Commands

Command	Description
application	Enables a voice application on a dial peer.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.
service	Loads and configures a specific, standalone application on a dial peer.
show call application voice	Displays information about voice applications.

call application cache reload time

Note Effective with Cisco IOS Release 12.3(14)T, the **call application cache reload time** command is replaced by the **cache reload time** command in application configuration global mode. See the **cache reload time** command for more information.

To configure the router to reload the Media Gateway Control Protocol (MGCP) scripts from cache on a regular interval, use the **call application cache reload time** command in global configuration mode. To set the value to the default, use the **no** form of this command.

call application cache reload time *bg-minutes*

no call application cache reload time

Syntax Description

bg-minutes	Specifies the number of minutes after which the background process is awakened. This background process checks the time elapsed since the script was last used and whether the script is current: • If the script has not been used in the last "unload time," it unloads the script and quits. The unload time is not configurable. • If the script has been used, the background process loads the script from the URL. It compares the scripts, and if they do not match, it begins using the new script for new calls.

Command Default 30 minutes

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.3(14)T	This command was replaced by the **cache reload time** command in application configuration global mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application cache reload 20

        Warning: This command has been deprecated. Please use the following:
             cache reload time
```

The following example displays the **call application cache reload time** command configured to specify 30 minutes before a background process is awakened:

```
call application cache reload time 30
```

Related Commands

Command	Description
cache reload time	Configures the router to reload scripts from cache on a regular interval.
call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
show call application voice	Displays all Tcl or MGCP scripts that are loaded.

call application dump event-log

To flush the event log buffer for application instances to an external file, use the **call application dump event-log** command in privileged EXEC mode.

call application dump event-log

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command immediately writes the event log buffer to the external file whose location is defined with the **call application event-log dump ftp** command in global configuration mode.

Note The **call application dump event-log** command and the **call application event-log dump ftp** command are two different commands.

Examples

The following example flushes the application event log buffer:

```
Router# call application dump event-log
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
call application event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
show call application session-level	Displays event logs and statistics for voice application instances.

call application event-log

Note Effective with Cisco IOS Release 12.3(14)T, the **call application event-log** command is replaced by the **event-log** command in application configuration monitor mode. See the **event-log** command for more information.

To enable event logging for all voice application instances, use the **call application event-log** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application event-log

no call application event-log

Syntax Description

This command has no arguments or keywords.

Command Default

Event logging for voice applications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **event-log** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command enables event logging globally for all voice application instances. To enable or disable event logging for a specific application, use the **call application voice event-log** command.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application event-log

        Warning: This command has been deprecated. Please use the following:
             event-log
```

The following example enables event logging for all application instances:

```
call application event-log
```

Related Commands

Command	Description
call application event-log error-only	Restricts event logging to error events only for application instances.
call application event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application stats	Enables statistics collection for voice applications.
call application voice event-log	Enables event logging for a specific voice application.
call leg event-log	Enables event logging for voice, fax, and modem call legs.
event-log	Enables event logging for applications.
monitor call application event-log	Displays the event log for an active application instance in real-time.
show call application session-level	Displays event logs and statistics for voice application instances.

call application event-log dump ftp

Note Effective with Cisco IOS Release 12.3(14)T, the **call application event-log dump ftp** command is replaced by the **event-log dump ftp** command in application configuration monitor mode. See the **event-log dump ftp** command for more information.

To enable the gateway to write the contents of the application event log buffer to an external file, use the **call application event-log dump ftp** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application event-log dump ftp *server*[**:***port*]*/file* **username** *username* **password** [*encryption-type*] *password*

no call application event-log dump ftp

Syntax Description

server	Name or IP address of FTP server where file is located.
:*port*	(Optional) Specific port number on server.
/file	Name and path of file.
username	Username required to access file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password	Password required to access file.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **event-log dump ftp** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command enables the gateway to automatically write the event log buffer to the named file either after an active application instance terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **call application event-log max-buffer-size** command. To manually flush the event log buffer, use the **call application dump event-log** command in privileged EXEC mode.

Note The **call application dump event-log** command and the **call application event-log dump ftp** command are two different commands.

Note Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application dump event-log

        Warning: This command has been deprecated. Please use the following:
             event-log dump ftp
```

The following example enables the gateway to write application event logs to an external file named app_elogs.log on a server named ftp-server:

```
call application event-log dump ftp ftp-server/:elogs/app-elogs.log username myname
password 0 mypass
```

The following example specifies that application event logs are written to an external file named app_elogs.log on a server with the IP address of 10.10.10.101:

```
call application event-log dump ftp 10.10.10.101/:elogs/app-elogs.log username myname
password 0 mypass
```

Related Commands

Command	Description
call application dump event-log	Flushes the event log buffer for application instances to an external file.
call application event-log	Enables event logging for voice application instances.
call application event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
show call application session-level	Displays event logs and statistics for voice application instances.

call application event-log error-only

Note Effective with Cisco IOS Release 12.3(14)T, the **call application event-log error-only** command is replaced by the **event-log error-only** command in application configuration monitor mode. See the **event-log error-only** command for more information.

To restrict event logging to error events only for application instances, use the **call application event-log error-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application event-log error-only

no call application event-log error-only

Syntax Description

This command has no arguments or keywords.

Command Default

All application events are logged.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **event-log error-only** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command limits new event logging to error events only; it does not enable logging. You must use this command with either the **call application event-log** command, which enables event logging for all voice applications, or with the **call application voice event-log** command, which enables event logging for a specific application. Any events logged before this command is issued are not affected.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application event-log error-only

        Warning: This command has been deprecated. Please use the following:
             event-log error-only
```

The following example enables event logging for error events only:

```
call application event-log
call application event-log error-only
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application history session event-log save-exception-only	Saves in history only the event logs for application instances that have at least one error.
call application voice event-log	Enables event logging for a specific voice application.
event-log error-only	Restricts event logging to error events only for application instances.
show call application app-level	Displays application-level statistics for voice applications.
show call application session-level	Displays event logs and statistics for voice application instances.

call application event-log max-buffer-size

Note Effective with Cisco IOS Release 12.3(14)T, the **call application event-log max-buffer-size** command is replaced by the **event-log max-buffer-size** command in application configuration monitor mode. See the **event-log max-buffer-size** command for more information.

To set the maximum size of the event log buffer for each application instance, use the **call application event-log max-buffer-size** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application event-log max-buffer-size *kilobytes*

no call application event-log max-buffer-size

Syntax Description

kilobytes	Maximum buffer size, in kilobytes. Range is 1 to 50. Default is 4.

Command Default 4 *kilobytes*

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **event-log max-buffer-size** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application session-level** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **call application event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **call application event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Note Do not set the maximum buffer size to more than you need for a typical application session. After an active session terminates, the amount of memory used by the buffer is allocated to the history table and is maintained for the length of time set by the **call application history session retain-timer** command. Also consider that most fatal errors are captured at the end of an event log.

To conserve memory resources, write the event log buffer to FTP by using the **call application event-log dump ftp** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application event-log max-buffer-size

        Warning: This command has been deprecated. Please use the following:
             event-log max-buffer-size
```

The following example sets the application event log buffer to 8 kilobytes:

```
call application event-log
call application event-log max-buffer-size 8
```

Related Commands

Command	Description
call application dump event-log	Flushes the event log buffer for application instances to an external file.
call application event-log	Enables event logging for voice application instances.
call application event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
show call application session-level	Displays event logs and statistics for voice application instances.

call application global

Note Effective with Cisco IOS Release 12.3(14)T, the **call application global** command is replaced by the **global** command in application configuration mode. See the **global** command for more information.

To configure an application to use for incoming calls whose incoming dial peer does not have an explicit application configured, use the **call application global** command in global configuration mode. To remove the application, use the **no** form of this command.

call application global *application-name*

no call application global *application-name*

Syntax Description

application-name	Character string that defines the name of the application.

Command Default

The default application is **default** for all dial peers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(14)T	This command was replaced by the **global** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

The application defined in the dial peer always takes precedence over the global application configured with the **call application global** command. The application configured with this command executes only when a dial peer has no application configured.

The application you configure with this command can be an application other than the default session application, but it must be included with the Cisco IOS software or be loaded onto the gateway with the **call application voice** command before using this command. If the application does not exist in Cisco IOS software or has not been loaded onto the gateway, this command will have no effect.

Note In Cisco IOS Release 12.3(4)T and later releases, the application-name default refers to the applicationCall Admission Control Based on CPU Utilization that supports Open Settlement Protocol (OSP), call transfer, and call forwarding. The default session application in Cisco IOS Release 12.2(13)T

and earlier releases has been renamed default.old.c and can still be configured for specific dial peers through the **application** command or globally configured for all inbound dial peers through the **call application global** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application global

        Warning: This command has been deprecated. Please use the following:
           global
```

In the following example, the clid_authen_collect application is configured as the global application for all inbound dial peers that do not have a specific application configured:

```
call application global clid_authen_collect
```

Related Commands

Command	Description
application	Enables a specific IVR application on a dial peer.
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
global	Enters application configuration mode.

call application history session event-log save-exception-only

Note Effective with Cisco IOS Release 12.3(14)T, the **call application history session event-log save-exception-only** command is replaced by the **history session event-log save-exception-only** command in application configuration monitor mode. See the **history session event-log save-exception-only** command for more information.

To save in history only the event logs for application sessions that have at least one error, use the **call application history session event-log save-exception-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application history session event-log save-exception-only

no call application history session event-log save-exception-only

Syntax Description

This command has no arguments or keywords.

Command Default

All event logs for sessions are saved to history.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **history session event-log save-exception-only** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Application event logs move from active to history after an instance terminates. If you use this command, the voice gateway saves event logs only for instances that had one or more errors. Event logs for normal instances that do not contain any errors are not saved to history.

Note This command does not affect records saved to an FTP server by using the **call application dump event-log** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application history session event-log save-exception-only

        Warning: This command has been deprecated. Please use the following:
             history session event-log save-exception-only
```

The following example saves an event log in history only if the instance had an error:

```
call application history session event-log save-exception-only
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application event-log error-only	Restricts event logging to error events only for application instances.
call application event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
call application history session max-records	Sets the maximum number of application instance records saved in history.
call application history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
history session event-log save-exception-only	Saves in history only the event logs for application sessions that have at least one error.

call application history session max-records

Note Effective with Cisco IOS Release 12.3(14)T, the **call application history session max-records** command is replaced by the **history session max-records** command in application configuration monitor mode. See the **history session max-records** command for more information.

To set the maximum number of application instance records saved in history, use the **call application history session max-records** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application history session max-records *number*

no call application history session max-records

Syntax Description

number	Maximum number of records to save in history. Range is 0 to 2000. Default is 360.

Command Default 360

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **history session max-records** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines This command affects the number of records that display when you use the **show call application history session-level** command.

Examples Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application history session max-records

        Warning: This command has been deprecated. Please use the following:
             history session max-records
```

The following example sets the maximum record limit to 500:

```
call application history session max-records 500
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application history session event-log save-exception-only	Saves in history only the event logs for application instances that have at least one error.
call application history session retain-timer	Sets the maximum number of minutes that application instance records are saved in history.
history session max-records	Sets the maximum number of application instance records saved in history.
show call application session-level	Displays event logs and statistics for voice application instances.

call application history session retain-timer

Note Effective with Cisco IOS Release 12.3(14)T, the **call application history session retain-timer** command is replaced by the **history session retain-timer** command in application configuration monitor mode. See the **history session retain-timer** command for more information.

To set the maximum number of minutes for which application instance records are saved in history, use the **call application history session retain-timer** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application history session retain-timer *minutes*

no **call application history session retain-timer**

Syntax Description

minutes	Maximum time, in minutes, for which history records are saved. Range is 0 to 4294,967,295. Default is 15.

Command Default 15

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **history session retain-timer** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines This command affects the number of records that display when you use the **show call application history session-level** command.

Examples Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application history session retain-timer

        Warning: This command has been deprecated. Please use the following:
             history session retain-timer
```

The following example sets the maximum time to save history records to 1 hour:

```
call application history session retain-timer 60
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application history session event-log save-exception-only	Saves in history only the event logs for application instances that have at least one error.
call application history session max-records	Sets the maximum number of application instance records saved in history.
history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
show call application session-level	Displays event logs and statistics for voice application instances.

call application interface dump event-log

To flush the event log buffer for application interfaces to an external file, use the **call application interface dump event-log** command in privileged EXEC mode.

call application interface dump event-log

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines This command immediately writes the event log buffer to the external file whose location is defined with the **call application interface event-log dump ftp** command in global configuration mode.

Note The **call application interface dump event-log** command and the **call application interface event-log dump ftp** command are two different commands.

Examples The following example writes the event log buffer to the external file named int_elogs:

```
Router(config)# call application interface event-log dump ftp ftp-server/int_elogs.log
username myname password 0 mypass
Router(config)# exit
Router# call application interface dump event-log
```

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface event-log dump ftp	Enables the voice gateway to write the contents of the interface event log buffer to an external file.
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface event-log

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface event-log** command is replaced by the **interface event-log** command in application configuration monitor mode. See the **interface event-log** command for more information.

To enable event logging for interfaces that provide services to voice applications, use the **call application interface event-log** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface event-log [{**aaa** | **asr** | **flash** | **http** | **ram** | **rtsp** | **smtp** | **tftp** | **tts**} [**server** *server*] [**disable**]]

no call application interface event-log [{**aaa** | **asr** | **flash** | **http** | **ram** | **rtsp** | **smtp** | **tftp** | **tts**} [**server** *server*] [**disable**]]

Syntax Description

aaa	Authentication, authorization, and accounting (AAA) interface type.
asr	Automatic speech recognition (ASR) interface type.
flash	Flash memory of the Cisco gateway.
http	Hypertext Transfer Protocol (HTTP) interface type.
ram	Memory of the Cisco gateway.
rtsp	Real Time Streaming Protocol (RTSP) interface type.
smtp	Simple Mail Transfer Protocol (SMTP) interface type.
tftp	Trivial File Transfer Protocol (TFTP) interface type.
tts	Text-to-speech (TTS) interface type.
server *server*	(Optional) Server name or IP address.
disable	(Optional) Disables event logging for the specified interface type or server.

Command Default Event logging for application interfaces is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface event-log** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command enables event logging globally for all interface types and servers unless you select a specific interface type or server. Specifying an interface type takes precedence over the global command for a specific interface type. Specifying an individual server takes precedence over the interface type.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface event-log

        Warning: This command has been deprecated. Please use the following:
             interface event-log
```

The following example enables event logging for all interfaces:

```
call application interface event-log
```

The following example enables event logging for HTTP interfaces only:

```
call application interface event-log http
```

The following example enables event logging for all interfaces except HTTP:

```
call application interface event-log
call application interface event-log http disable
```

The following example enables event logging for all HTTP servers except the server with the IP address of 10.10.1.1:

```
call application interface event-log http
call application interface event-log http server http://10.10.1.1 disable
```

Related Commands

Command	Description
call application interface event-log dump ftp	Enables the gateway to write the contents of the interface event log buffer to an external file.
call application interface event-log error-only	Restricts event logging to error events only for application interfaces.
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
call application interface max-server-records	Sets the maximum number of application interface records that are saved.
call application interface stats	Enables statistics collection for application interfaces.
interface event-log	Enables event logging for interfaces providing services to voice applications.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface event-log dump ftp

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface event-log dump ftp** command is replaced by the **interface event-log dump ftp** command in application configuration monitor mode. See the **interface event-log dump ftp** command for more information.

To enable the gateway to write the contents of the interface event log buffer to an external file, use the **call application interface event-log dump ftp** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface event-log dump ftp *server*[**:***port*]*/file* **username** *username* **password** [*encryption-type*] *password*

no call application interface event-log dump ftp

Syntax Description

server	Name or IP address of FTP server where the file is located.
:*port*	(Optional) Specific port number on server.
/file	Name and path of file.
username *username*	Username required to access file.
encryption-type	(Optional) Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password *password*	Password required to access file.

Command Default Interface event log buffer is not written to an external file.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface event-log dump ftp** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines This command enables the gateway to automatically write the interface event log buffer to the named file when the buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **call application interface event-log max-buffer-size** command. To manually flush the event log buffer, use the **call application interface dump event-log** command in privileged EXEC mode.

Note

- The **call application interface dump event-log** command and the **call application interface event-log dump ftp** command are two different commands.
- Enabling the gateway to write event logs to FTP can adversely impact gateway-memory resources in scenarios such as the following:
  - The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
  - The designated FTP server is not powerful enough to perform FTP transfers quickly
  - Bandwidth on the link between the gateway and the FTP server is not large enough
  - The gateway is receiving a high volume of short-duration calls or calls that are failing

  You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface event-log dump ftp

        Warning: This command has been deprecated. Please use the following:
           interface event-log dump ftp
```

The following example specifies that interface event log are written to an external file named int_elogs.log on a server named ftp-server:

```
call application interface event-log dump ftp ftp-server/elogs/int_elogs.log username
myname password 0 mypass
```

The following example specifies that application event logs are written to an external file named int_elogs.log on a server with the IP address of 10.10.10.101:

```
call application interface event-log dump ftp 10.10.10.101/elogs/int_elogs.log username
myname password 0 mypass
```

Related Commands

Command	Description
call application interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
call application interface max-server-records	Sets the maximum number of application interface records that are saved.
interface event-log dump ftp	Enables the gateway to write the contents of the interface event log buffer to an external file.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface event-log error-only

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface event-log error-only** command is replaced by the **interface event-log error only** command in application configuration monitor mode. See the **interface event-log error only** command for more information.

To restrict event logging to error events only for application interfaces, use the **call application interface event-log error-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface event-log error-only

no call application interface event-log error-only

Syntax Description

This command has no arguments or keywords.

Command Default

All events are logged.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface event-log error only** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command limits the severity level of the events that are logged; it does not enable logging. You must use this command with the **call application interface event-log** command, which enables event logging for all application interfaces.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface event-log error-only

        Warning: This command has been deprecated. Please use the following:
             interface event-log error only
```

The following example enables event logging for error events only:

```
call application interface event-log error-only
```

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
call application interface max-server-records	Sets the maximum number of application interface records that are saved.
interface event-log error-only	Restricts event logging to error events only for application interfaces.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface event-log max-buffer-size

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface event-log max-buffer-size** command is replaced by the **interface event-log max-buffer-size** command in application configuration monitor mode. See the **interface event-log max-buffer-size** command for more information.

To set the maximum size of the event log buffer for each application interface, use the **call application interface event-log max-buffer-size** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface event-log max-buffer-size *kilobytes*

no call application interface event-log max-buffer-size

Syntax Description

kilobytes	Maximum buffer size, in kilobytes. Range is 1 to 10. Default is 4.

Command Default 4 kilobytes

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface event-log max-buffer-size** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application interface** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **call application interface event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **call application interface event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface event-log max-buffer-size

        Warning: This command has been deprecated. Please use the following:
           interface event-log max-buffer-size
```

The following example sets the maximum buffer size to 8 kilobytes:

```
call application interface event-log max-buffer-size 8
```

Related Commands

Command	Description
call application interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
call application interface event-log dump ftp	Enables the gateway to write the contents of the interface event log buffer to an external file.
call application interface max-server-records	Sets the maximum number of application interface records that are saved.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface max-server-records

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface max-server-records** command is replaced by the **interface max-server-records** command in application configuration monitor mode. See the **interface max-server-records** command for more information.

To set the maximum number of application interface records that are saved, use the **call application interface max-server-records** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface max-server-records *number*

no call application interface max-server-records

Syntax Description

number	Maximum number of records to save. Range is 1 to 100. Default is 10.

Command Default 10

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface max-server-records** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines Only the specified number of records from the most recently accessed servers are kept.

Examples Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface max-server-records

        Warning: This command has been deprecated. Please use the following:
             interface max-server-records
```

The following example sets the maximum saved records to 50:

```
call application interface max-server-records 50
```

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

call application interface stats

Note Effective with Cisco IOS Release 12.3(14)T, the **call application interface stats** command is replaced by the **interface stats** command in application configuration monitor mode. See the **interface stats** command for more information.

To enable statistics collection for application interfaces, use the **call application interface stats** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application interface stats

no call application interface stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **interface stats** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

To display the interface statistics enabled by this command, use the **show call application interface** command. To reset the interface counters to zero, use the **clear call application interface** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application interface stats

        Warning: This command has been deprecated. Please use the following:
             interface stats
```

The following example enables statistics collection for application interfaces:

```
call application interface stats
```

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
clear call application interface	Clears application interface statistics or event logs.
interface stats	Enables statistics collection for application interfaces.
show call application interface	Displays event logs and statistics for application interfaces.
stats	Enables statistics collection for voice applications.

call application session start (global)

Note Effective with Cisco IOS Release 12.3(14)T, the **call application session start** (global) command is replaced by the the **session start** command in application configuration mode. See the **session start** command for more information.

To start a new instance (session) of a Tcl IVR 2.0 application, use the **call application session start** command in global configuration mode. To stop the session and remove the configuration, use the **no** form of this command.

call application session start *instance-name application-name*

no call application session start *instance-name*

Syntax Description

instance-name	Alphanumeric label that uniquely identifies this application instance.
application-name	Name of the Tcl application. This is the name of the application that was assigned with the **call application voice** command.

Command Default

This command has no default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(14)T	The **call application session start** (global configuration) command was replaced by the **session start** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command starts a new session, or instance, of a Tcl IVR 2.0 application. It cannot start a session for a VoiceXML application because Cisco IOS software cannot start a VoiceXML application without an active call leg.

You can start an application instance only after the Tcl application is loaded onto the gateway with the **call application voice** command.

If this command is used, the session restarts if the gateway reboots.

The **no call application session start** command stops the Tcl session and removes the configuration from the gateway. You can stop an application session without removing the configuration by using the **call application session stop** command.

VoiceXML sessions cannot be stopped with the **no call application session start** command because VoiceXML sessions cannot be started with Cisco IOS commands.

If the application session stops running, it does not restart unless the gateway reboots. A Tcl script might intentionally stop running by executing a “call close” command for example, or it might fail because of a script error.

You can start multiple instances of the same application by using different instance names.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application session start

        Warning: This command has been deprecated. Please use the following:
             session start
```

The following example starts a session named my_instance for the application named demo:

```
call application session start my_instance demo
```

The following example starts another session for the application named demo:

```
call application session start my_instance2 demo
```

Related Commands

Command	Description
call application session start (privileged EXEC)	Starts a new instance (session) of a Tcl application from privileged EXEC mode.
call application session stop	Stops a voice application session that is running.
debug voip ivr	Displays debug messages for VoIP IVR interactions.
session start	Starts a new instance (session) of a Tcl IVR 2.0 application.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

call application session start (privileged EXEC)

To start a new instance (session) of a Tcl IVR 2.0 application, use the **call application session start** command in privileged EXEC mode.

call application session start *instance-name* [*application-name*]

Syntax Description

instance-name	Alphanumeric label that uniquely identifies this application instance.
application-name	(Optional) Name of the Tcl application. This is the name of the application that was assigned with the **call application voice** command. **Note** This argument is optional if the application instance was previously started and stopped.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command starts a new session, or instance, of a Tcl IVR 2.0 application. It cannot start a session for a VoiceXML application because Cisco IOS software cannot start a VoiceXML application without an active call leg.

You can start an application instance only after the Tcl application is loaded onto the gateway with the **call application voice** command.

Using this command does not restart the session if the gateway reboots. To automatically restart the session if the gateway reboots, use the **call application session start** command in global configuration mode.

To stop an application session once it starts running, use the **call application session stop** command.

If the application session stops running, it does not restart unless the gateway reboots and the **call application session start** command is used in global configuration mode. A Tcl script might intentionally stop running by executing a “call close” command for example, or it might fail due to a script error.

You can start multiple instances of the same application by using different instance names.

Examples

The following example restarts an application session called my_instance:

```
call application session start my_instance
```

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a Tcl application in global configuration mode.
call application session stop	Stops a voice application session that is running.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

call application session stop

To stop a voice application session that is running, use the **call application session stop** command in privileged EXEC mode.

call application session stop {**callid** *call-id* | **handle** *handle* | **id** *session-id* | **name** *instance-name*}

Syntax Description

callid *call-id*	Call-leg ID that can be displayed in the output from the **debug voip ivr script** command if the Tcl script uses puts commands.
handle *handle*	Handle of a session from the Tcl mod_handle infotag.
id *session-id*	Session ID that can be displayed with the **show call application sessions** command.
name *instance-name*	Instance name that was configured with the **call application session start** command.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command stops a Tcl IVR 2.0 or VoiceXML application session that is identified by one of four different methods: call ID, handle, session ID, or instance name. To see a list of currently running applications, use the **show call application sessions** command.

A Tcl session that is stopped with this command receives a session terminate event. The session is expected to close all call legs and stop. If a session does not close itself after a 10-second timer, it is forcibly stopped and all call legs that it controls disconnect.

Using this command to stop a VoiceXML session immediately stops the document interpretation and disconnects the call leg. No VoiceXML events are thrown.

If you stop a Tcl session that is configured to start with the **call application session start** command in global configuration mode, you must remove the session by using the **no call application session start** command before you can restart it.

To see a list of stopped sessions, use the **show call application sessions** command. Only stopped sessions that are configured to start with the **call application session start** command in global configuration mode are displayed. If a session was started with the **call application session start** command in privileged EXEC mode, it is not tracked by the system and it is not shown as stopped in the output of the **show call application sessions** command.

Examples

The following example stops an application session called my_instance:

```
call application session stop name my_instance
```

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a Tcl application from global configuration mode.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

call application stats

Note Effective with Cisco IOS Release 12.3(14)T, the **call application stats** command is replaced by the **stats** command in application configuration monitor mode. See the **stats** command for more information.

To enable statistics collection for voice applications, use the **call application stats** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application stats

no call application stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **stats** command in application configuration monitor mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

To display the application statistics, use the **show call application session-level**, **show call application app-level**, or **show call application gateway-level** command. To reset the application counters in history to zero, use the **clear call application stats** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application stats

        Warning: This command has been deprecated. Please use the following:
             stats
```

The following example enables statistics collection for voice applications:

```
call application stats
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application interface stats	Enables statistics collection for application interfaces.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.
stats	Enables statistics collection for voice applications.

call application voice

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice** command is replaced by the commands shown in Table 2. See these commands for more information.

To define the name of a voice application and specify the location of the Tool Command Language (Tcl) or VoiceXML document to load for this application, use the **call application voice** command in global configuration mode. To remove the defined application and all configured parameters associated with it, use the **no** form of this command.

call application voice *application-name* {*location* | *av-pair*}

no call application voice *application-name*

Syntax Description

application-name	Character string that defines the name of the voice application.
location	Location of the Tcl script or VoiceXML document in URL format. Valid storage locations are TFTP, FTP, HTTP, and flash memory.
av-pair	Text string that defines attribute-value (AV) pairs specified by the Tcl script and understood by the RADIUS server. Multiple AV pairs can be enclosed in quotes; up to 512 entries are supported.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XH	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T. The *location* argument was added.
12.1(3)T	The *av-pair* argument was added for AV pairs.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	This command was modified to support VoiceXML applications and HTTP server locations on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(4)XM	This command was implemented on the Cisco 1751. Support for other Cisco platforms is not included in this release.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 3725, Cisco 3745, and Cisco 7200 series.
12.2(11)T	This command was implemented for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.2(15)T	MCID AV-pairs were added for the *av-pair* argument; they are mcid-dtmf, mcid-release-timer, and mcid-retry-limit.
12.3(8)T	Support was added to allow up to 512 multiple AV pairs (enclosed in quotes) to be used in a single command.
12.3(14)T	This command was replaced. The **call application voice** command was replaced by the commands shown in Table 2.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

The **call application voice** command was replaced by the commands shown in Table 2.

Table 2 call application voice Command Replacements

Command	Command Mode	Purpose
application	Global configuration	Enters application configuration mode to configure voice applications and services.
service	Application configuration	Enters service configuration mode to configure a standalone application, such as a debit card script.
package	Application configuration	Use to load and configure a package. A package is a linkable set of C or Tcl functions that provide functionality invoked by applications or other packages.
param	Application parameter configuration	Use to configure parameters for services or packages.

Use this command when configuring interactive voice response (IVR) or one of the IVR-related features (such as Debit Card) to define the name of an application and to identify the location of the Tcl script or VoiceXML document associated with the application.

A voice application must be configured by using this command before the application can be configured with the **application** command in a dial peer.

Tcl scripts and VoiceXML documents can be stored in any of the following locations: on TFTP, FTP, or HTTP servers, in the flash memory of the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations, and on Real-Time Streaming Protocol (RTSP) servers.

HTTP is the recommended protocol for loading applications and audio prompts because of its efficient design for loading information over the web. For example, it has methods for determining how long a file can be cached and whether a cached file is still valid.

Include the file type extension in the filename (.vxml or .tcl) when specifying the document used by the application. Tcl files require the extension .tcl, and VoiceXML documents require .vxml.

Note The **no call application voice** command causes all related call application commands—for instance, **call application voice language** and **call application voice set-location**—to be deleted. The **no call application voice** *application-name* command removes the entire application and all parameters, if configured.

Examples

Effective with Cisco IOS Release 12.3(14)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice

        Warning: This command has been deprecated. Please use the following:
             application
               service
                 package
                   param
```

The following example defines the fax-relay application and the TFTP server location of the associated Tcl script:

```
call application voice fax-relay tftp://keyer/faxrelay.tcl
```

The following example defines the application “prepaid” and the TFTP server location of the associated Tcl script:

```
call application voice prepaid tftp://keyer/debitcard.tcl
```

The following is an example of AV pair configuration:

```
set avsend(h323-ivr-out,)) "payphone:true"
set avsend(323-ivr-out,1) "creditTime:3400"
```

The AV pair (after the array is defined, as in the prior example) must be sent to the server using the authentication, authorization, and accounting (AAA) authenticate or AAA authorize verbs as follows:

```
aaa authenticate $account $password $avsend
```

The script would use this AV pair whenever it is needed to convey information to the RADIUS server that cannot be represented by the standard vendor-specific attributes (VSAs).

The following example shows how to define the VoiceXML application “vapptest1” and the flash memory location of the associated VoiceXML document “demo0.vxml”:

```
call application voice vapptest1 flash:demo0.vxml
```

The following example specifies the MCID application name, the TFTP server location of the associated Tcl script, and the AV-pairs associated with the MCID application:

```
call application voice mcid tftp://keyer/app_mcid.2.0.0.40.tcl
call application voice mcid mcid-dtmf #99
call application voice mcid-retry-limit 3
call application voice mcid mcid-release-timer 90
```

Related Commands

Command	Description
application (dial peer)	Defines the call application in the dial peer.
application (global configuation)	Enters application configuration mode to configure applications.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script or VoiceXML document.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice security trusted	Sets the security level of a VoiceXML application to trusted so that ANI is not blocked.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
package	Enters application parameter configuration mode to load and configure a package.
param	Loads and configures parameters in a package or a service (application) on the gateway.
service	Loads and configures a specific, standalone application on a dial peer.
show call application voice	Displays information about voice applications.

call application voice access-method

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice access-method** command was replaced by the **param access-method** command in application parameter configuration mode. See the **param access-method** command for more information.

To specify the access method for two-stage dialing for the designated application, use the **call application voice access-method** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

call application voice *application-name* **access-method** {**prompt-user** | **redialer**}

no call application voice *application-name* **access-method**

Syntax Description

application-name	Name of the application.
prompt-user	Specifies that no DID is set in the incoming POTS dial peer and that a Tcl script in the incoming POTS dial peer is used for two-stage dialing.
redialer	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device are used for two-stage dialing.

Command Default Prompt-user (when DID is not set in the dial peer)

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into the Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was introduced on the Cisco 1750.
12.3(14)T	This command was replaced by the **param access-method** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines Use the **call application voice access-method** command to specify the access method for two-stage dialing when DID is disabled in the POTS dial peer.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice access-method

        Warning: This command has been deprecated. Please use the following:
             param access-method
```

The following example specifies prompt-user as the access method for two-stage dialing for the app_libretto_onramp9 IVR application:

```
call application voice app_libretto_onramp9 access-method prompt-user
```

Related Commands

Command	Description
call application voice	Loads a specified application onto the router from the TFTP server and gives it an application name by which it is known on the router.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param access-method	Specifies the access method for two-stage dialing for the designated application.

call application voice account-id-method

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice account-id-method** command is replaced by the **param account-id-method** command in application parameter configuration mode. See the **param account-id-method** command for more information.

To configure the fax detection IVR application to use a particular method to assign the account identifier, use the **call application voice account-id-method** command in global configuration mode. To remove configuration of this account identifier, use the **no** form of this command.

call application voice *application-name* **account-id-method** {**none** | **ani** | **dnis** | **gateway**}

no call application voice *application-name* **account-id-method**

Syntax Description

application-name	Name of the defined fax detection IVR application.
none	Account identifier is blank. This is the default.
ani	Account identifier is the calling party telephone number (automatic number identification, or ANI).
dnis	Account identifier is the dialed party telephone number (dialed number identification service, or DNIS).
gateway	Account identifier is a router-specific name derived from the hostname and domain name, displayed in the following format: router-name.domain-name.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced for the Cisco AS5300.
12.2(2)XB	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the Cisco AS5300, the Cisco AS5350, and Cisco AS5400.
12.3(14)T	This command was replaced by the **param account-id-method** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

When an on-ramp application converts a fax into an e-mail, the e-mail contains a field called x-account-id, which can be used for accounting or authentication. The x-account-id field can contain information supplied as a result of this command, such as the calling party's telephone number (**ani**), the called party's telephone number (**dnis**), or the name of the gateway (**gateway**).

This command is not supported by Cisco IOS help; that is, if you type **the call application voice fax_detect account-id-method command and a question mark (?)**, the Cisco IOS help does not supply a list of entries that are valid in place of the question mark.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application fax_detect account-id-method gateway

        Warning: This command has been deprecated. Please use the following:
             param account-id-method
```

The following example sets the fax detection IVR application account identifier to the router-specific name derived from the hostname and domain name:

```
call application voice fax_detect account-id-method gateway
```

Related Commands

Command	Description
call application voice	Loads a specified IVR application onto the router from the TFTP server and gives it an application name by which it is known on the router.
call application voice fax-dtmf	Configures the fax detection IVR application to recognize a specified digit that indicates a fax call in default-voice and default-fax modes.
call application voice mode	Configures the fax detection IVR application to operate in one of its four modes.
call application voice prompt	Configures the fax detection IVR application to use the specified audio file as a user prompt in listen-first mode, default-voice mode, or default-fax mode.
call application voice voice-dtmf	Configures the fax detection IVR application to recognize a specified digit that indicate a voice call in default-voice and default-fax modes.
param account-id-method	Configures an application to use a particular method to assign the account identifier.

call application voice authentication enable

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice authentication enable** command is replaced by the **param authentication enable** command in application configuration mode. See the **param authentication enable** command for more information.

To enable authentication, authorization, and accounting (AAA) services for a Tool Command Language (TCL) application, use the **call application voice authentication enable** command in global configuration mode. To disable authentication for a TCL application, use the **no** form of this command.

call application voice *application-name* **authentication enable**

no call application voice *application-name* **authentication enable**

Syntax Description

application-name	Name of the application.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.3(14)T	This command was replaced by the **param authentication enable** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines This command enables AAA authentication services for a TCL application if a AAA authentication method list has been defined using both the **aaa authentication** command and the **call application voice authen-list** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice authentication enable

        Warning: This command has been deprecated. Please use the following:
           param authentication enable
```

The following example enables a AAA authentication method list (called “sample”) to be used with outbound store-and-forward fax.

```
call application voice app_eaample_onramp9 authen-list sample
call application voice app_example_onramp9 authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
call application voice authen-list	Specifies the name of an authentication method list for a TCL application.
call application voice authen-method	Specifies the authentication method for a TCL application.

call application voice accounting-list

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice accounting-list** command is replaced by the **param accounting-list** in application configuration mode. See the **param accounting-list** command for more information.

To define the name of the accounting method list to be used for authentication, authorization, and accounting (AAA) with store-and-forward fax on a voice feature card (VFC), use the **call application voice accounting-list** command in global configuration mode. To undefine the accounting method list, use the **no** form of this command.

call application voice *application-name* **accounting-list** *method-list-name*

no call application voice *application-name* **accounting-list** *method-list-name*

Syntax Description

application-name	Name of the application.
method-list-name	Character string used to name a list of accounting methods to be used with store-and-forward fax.

Command Default No AAA accounting method list is defined

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.3(14)T	This command was replaced by the **param accounting-list** in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists that are used in store-and-forward fax are applied globally.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store-and-forward fax functions on VFCs. The command is not used on modem cards.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice accounting-list

        Warning: This command has been deprecated. Please use the following:
           param accounting-list
```

The following example defines a AAA accounting method list “example” to be used with store-and-forward fax:

```
aaa new-model
call application voice app_libretto_onramp9 accounting-list example
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
call application voice accounting enable	Enables AAA accounting for a TCL application.
mmoip aaa receive-accounting enable	Enables on-ramp AAA accounting services.

call application voice accounting-template

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice accounting-template** command is obsolete. Use the **call accounting-template** command in application configuration mode to configure a voice accounting template.

To configure T.37 fax accounting with VoIP authentication, authorization, and accounting (AAA) nonblocking Application Programming Interface (API), use the **call application voice accounting-template** command in global configuration mode. To remove the defined application and all configured parameters associated with it, use the **no** form of this command.

call application voice *application-name* **accounting-template** *template-name*

no call application voice *application-name* **accounting-template** *template-name*

Syntax Description

application-name	Defines the name of the T.37 voice application. • Use the **call application voice** command to define the name of a voice application and specify the location of the Tool Command Language (Tcl) or VoiceXML document to load for this application.
template-name	Defines the name of the template. • Use the **call accounting-template voice** command to define the template name.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(14)T	This command is obsolete. Use the **call accounting-template** command in application configuration mode to configure a voice accounting template.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command enables T.37 fax to be consistent with VoIP AAA accounting services, which uses the Cisco IOS software nonblocking APIs. This command creates accounting templates for faxes by associating the template name with the T.37 onramp or offramp application.

You can define an accounting template to specify information that is included in an accounting packet.

Note This command applies only to T.37 fax.

Use the **show call active fax** and the **show call history fax** commands to check the configuration.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice accounting-template

        Warning: This command has been deprecated. Please use the following:
             call accounting-template
```

The following is an example configuration using the T.37 accounting template:

```
Router(config)# call application voice t37_onramp accounting-template sample-name
Router(config)# call application voice t37_offramp accounting-template sample-name
```

Related Commands

Command	Description
application	Defines the call application in the dial peer.
call accounting-template	Selects an accounting template at a specific location.
call accounting-template voice	Selects an accounting template at a specific location.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script or VoiceXML document.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice security trusted	Sets the security level of a VoiceXML application to trusted so that ANI is not blocked.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
show call active fax	Displays call information for fax transmissions in progress.
show call application voice	Displays information about voice applications.
show call history fax	Displays the call history table for fax transmissions.

call application voice authen-list

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice authen-list** command was replaced by the **param authen-list** command in application configuration mode. See the **param authen-list** command for more information.

To specify the name of an authentication method list for a Tool Command Language (Tcl) application, use the **call application voice authen-list** command in global configuration mode. To disable the authentication method list for a Tcl application, use the **no** form of this command.

call application voice *application-name* **authen-list** *method-list-name*

no call application voice *application-name* **authen-list** *method-list-name*

Syntax Description

application-name	Name of the application.
method-list-name	Character string used to name a list of authentication methods to be used with T.38 fax relay and T.37 store-and-forward fax.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.3(14)T	This command was replaced by the **param authen-list** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command defines the name of the authentication, authorization, and accounting (AAA) method list to be used with fax applications on voice feature cards. The method list itself, which defines the type of authentication services provided for store-and-forward fax, is defined using the **aaa authentication** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), AAA method lists that are used with fax applications are applied globally.

After the authentication method lists have been defined, they are enabled by using the **call application voice authentication enable** command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice authen-list

        Warning: This command has been deprecated. Please use the following:
           param authen-list
```

The following example defines a AAA authentication method list (called “fax”) to be used with T.38 fax relay and T.37 store-and-forward fax:

```
call application voice app_libretto_onramp9 authen-list fax
```

Related Commands

Command	Description
aaa authentication	Enable AAA accounting of requested services for billing or security purposes.
call application voice authen-method	Specifies the authentication method for a Tcl application.
call application voice authentication enable	Enables AAA authentication services for a Tcl application.

call application voice authen-method

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice authen-method** command is replaced by the **param authen-method** command in application configuration mode. See the **param authen-method** command for more information.

To specify an authentication, authorization, and accounting (AAA) authentication method for a Tool Command Language (Tcl) application, use the **call application voice authen-method** command in global configuration mode. To disable the authentication method for a Tcl application, use the **no** form of this command.

call application voice *application-name* **authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

no call application voice *application-name* **authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

application-name	Name of the application.
prompt-user	User is prompted for the Tcl application account identifier.
ani	Calling party telephone number (automatic number identification or ANI) is used as the Tcl application account identifier.
dnis	Called party telephone number (dialed number identification service or DNIS) is used as the Tcl application account identifier.
gateway	Router-specific name derived from the host name and domain name is used as the Tcl application account identifier, displayed in the following format: *router-name.domain-name*.
redialer-id	Account string returned by the external redialer device is used as the Tcl application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer-dnis	Called party telephone number (dialed number identification service or DNIS) is used as the Tcl application account identifier captured by the redialer if a redialer device is present.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Release	Modification
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.3(14)T	This command was replaced by the **param authen-method** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Normally, when AAA is used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With T.37 store-and-forward fax and T.38 real-time fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication or that the user be prompted for the Tcl application.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice authen-method

        Warning: This command has been deprecated. Please use the following:
           param authen-method
```

The following example configures the router-specific name derived from the hostname and domain name as he Tcl application account identifier for the app_sample_onramp9 Tcl application:

```
call application voice app_sample_onramp9 authen-method gateway
```

Related Commands

Command	Description
call application voice authentication enable	Enables AAA authentication services for a Tcl application.
call application voice authen-list	Specifies the name of an authentication method list for a Tcl application.

call application voice accounting enable

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice accounting enable** command is replaced by the **param accounting enable** command in application configuration mode. See the **param accounting enable** command for more information.

To enable authentication, authorization, and accounting (AAA) accounting for a Tool Command Language (Tcl) application, use the **call application voice accounting enable** command in global configuration mode. To disable accounting for a Tcl application, use the **no** form of this command.

call application voice *application-name* **accounting enable**

no call application voice *application-name* **accounting enable**

Syntax Description

application-name	Name of the application.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.3(14)T	This command was replaced by the **param accounting enable** command in application configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command enables AAA accounting services if a AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice accounting enable

        Warning: This command has been deprecated. Please use the following:
           param accounting enable
```

The following example enables AAA accounting to be used with outbound store-and-forward fax:

```
call application voice app_libretto_onramp9 accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

call application voice default disc-prog-ind-at-connect

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice default disc-prog-ind-at-connect** command is replaced. Use one of the following commands:

- **param convert-discpi-after-connect** (application parameter configuration mode)
- **paramspace session_xwork convert-discpi-after-connect** (service configuration mode)

To convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state, use the **call application voice default disc-prog-ind-at-connect** command in global configuration mode. To revert to a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) when the call is in the active state, use the **no** form of this command.

call application voice default disc-prog-ind-at-connect [**1** | **0**]

no call application voice default disc-prog-ind-at-connect [**1** | **0**]

Syntax Description

1	(Optional) Convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
0	(Optional) Revert to a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Default

The DISCONNECT message has Progress Indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(14)T	The **call application voice default disc-prog-ind-at-connect** command was replaced. Use one of the following commands: • **param convert-discpi-after-connect** (application parameter configuration mode) • **paramspace session_xwork convert-discpi-after-connect** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command has no effect if the call is not in the active state.

This command is available for the default voice application. It may not be available when using some Tcl IVR applications.

The Cisco IOS command-line interface command completion and help features do not work with this command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice default disc-prog-ind-at-connect

        Warning: This command has been deprecated. Please use the following:
           param convert-discpi-after-connect
               paramspace session_xwork convert-discpi-after-connec
```

In the following example, a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) is converted to a regular DISCONNECT message when the call is in the active state:

```
call application voice default disc-prog-ind-at-connect 1
```

Related Commands

Command	Description
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
paramspace session_xwork convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

call application voice dsn-script

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice dsn-script** command is replaced by the **param dsn-script** command in application parameter configuration mode.

To specify the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp delivery status notification (DSN) and message disposition notification (MDN) e-mail messages, use the **call application voice dsn-script** command in global configuration mode. To remove the application, use the **no** form of this command.

call application voice *mail-application-name* **dsn-script** *application-name*

no call application voice *mail-application-name* **dsn-script** *application-name*

Syntax Description

mail-application-name	Name of the off-ramp mail application that launches the app_voicemail_offramp.tcl script when the gateway receives an e-mail trigger.
application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(14)T	This command was replaced by the **param dsn-script** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines When the off-ramp gateway receives a DSN or MDN e-mail message, it handles it in the same way as a voice e-mail trigger message. The dial peer is selected on the basis of dialed number identification service (DNIS), and the mail application hands off the call to the VoiceXML application that is configured with this command.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice dsn-script

        Warning: This command has been deprecated. Please use the following:
           param dsn-script
```

The following example shows how to define the DSN application and how to apply it to a dial peer:

```
call application voice offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
call application voice dsn-mapp-test tftp://sample/tftp-users/vxml/dsn-mapp-test.vxml
call application voice offramp-mapp dsn-script dsn-mapp-test
!
dial-peer voice 1000 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
application	Defines a specific voice application in the dial peer.
call application voice	Defines the name of a voice application and specifies the location of the document (Tcl or VoiceXML) to load for the application.
param dsn-script	Specifies the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp DSN and MDN e-mail messages.
show call application voice	Displays information about the configured voice applications.

call application voice event-log

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice event-log** is obsolete. To enable event logging for a specific voice application, use one of the following commands:

- **param event-log** (application parameter configuration mode)
- **paramspace appcommon event-log** (service configuration mod

To enable event logging for a specific voice application, use the **call application voice event-log** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application voice *application-name* **event-log** [**disable**]

no call application voice *application-name* **event-log**

Syntax Description

application-name	Name of the voice application.
disable	(Optional) Disables event logging for the named application.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	The **call application voice event-log** is obsolete. To enable event logging for a specific voice application, use one of the following commands: • **param event-log** (application parameter configuration mode) • **paramspace appcommon event-log** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command is application-specific; it takes precedence over the global configuration command, **call application event-log**, which enables event logging for all voice applications.

Before you can use this command, you must configure the named application on the gateway by using the **call application voice** command.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20 percent, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30 percent. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call call application voice event-log
       Warning: This command has been deprecated. Please use the following:
           param event-log
               paramspace appcommon event-log
```

The following example enables event logging for all instances of the application named sample_app:

```
call application voice sample_app event-log
```

The following example enables event logging for all applications except the application sample_app:

```
call application event-log
call application voice sample_app event-log disable
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
call application voice	Defines the name of a voice application and specifies the location of the script to load for the application.
monitor call application event-log	Displays the event log for an active application instance in real-time.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
paramspace appcommon event-log	Enable or disables logging for a service (application).
show call application session-level	Displays event logs and statistics for voice application instances.

call application voice fax-dtmf

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice fax-dtmf** command is replaced by the **param fax-dtmf** command in application parameter configuration mode. See the **param fax-dtmf** command for more information.

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes, use the **call application voice fax-dtmf** command in global configuration mode. To remove configuration of this digit, use the **no** form of this command.

call application voice *application-name* **fax-dtmf** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

no call application voice *application-name* **fax-dtmf** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

Syntax Description

application-name	The name of the fax detection IVR application that you defined when you loaded the application on the router.
0 | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**	The telephone keypad digit processed by the calling party to indicate a fax call, in response to the audio prompt that plays during the default-voice or default-fax mode of the fax detection IVR application.

Command Default **2**

Command Modes Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced for the Cisco AS5300.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(14)T	This command was replaced by the **param fax-dtmf** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode as defined by the **call application voice mode** command.

Only one digit can be specified in this command, and that digit must be different from the digit specified in the **call application voice voice-dtmf** command. You are not notified immediately if you make the error of configuring them both to the same digit. To find this error, you must start the debugging with the **debug voip ivr script** command and then observe some failing calls.

This command is not supported by Cisco IOS help; that is, if you type **call application voice fax_detect fax-dtmf and a question mark (?)**, Cisco IOS help does not supply a list of entries that are valid in place of the question mark.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice fax-dtmf

        Warning: This command has been deprecated. Please use the following:
           param fax-dtmf
```

The following example selects DTMF digit 1 to indicate a fax call:

```
call application voice fax_detect script_url
call application voice fax_detect fax-dtmf 1
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice	Loads an IVR application onto a router and gives it an application name.
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
call application voice mode	Configures the fax detection IVR application to operate in one of its four modes.
call application voice prompt	Configures the fax detection IVR application to use the specified audio file as a user prompt.
call application voice voice-dtmf	Configures the fax detection IVR application to recognize the specified digit to indicate a voice call.
debug voip ivr script	Displays debug information from the fax detection IVR script.
param fax-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes.

call application voice global-password

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice global-password** command is replaced by the **param global-password** command in application parameter configuration mode. See the **param global-password** command for more information.

To define a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card, use the **call application voice global-password** command in global configuration mode. To restore the default value, use the **no** form of this command.

call application voice *application-name* **global-password** *password*

no call application voice *application-name* **global-password** *password*

Syntax Description

application-name	The name of the application.
password	Character string used to define the CiscoSecure for Windows NT password to be used with store-and-forward fax. The maximum length is 64 alphanumeric characters.

Command Default No password is defined

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.3(14)T	This command is replaced by the **param global-password** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines CiscoSecure for Windows NT might require a separate password to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Windows NT server use this defined password.

This command applies to on-ramp store-and-forward fax functions on Cisco AS5300 universal access server voice feature cards. It is not used on modem cards.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice global-password

        Warning: This command has been deprecated. Please use the following:
           param global-password
```

The following example shows a password (abercrombie) being used by AAA for the app_sample_onramp9 Tcl application:

```
call application voice app_sample_onramp9 global-password abercrombie
```

Related Commands

Command	Description
param global-password	Defines a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card.

call application voice language

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice language** is replaced by the following commands:

- **param language** (application parameter configuration mode)
- **paramspace language** (service configuration mode)

See these commands for more information.

To specify the language for dynamic prompts used by an interactive voice response (IVR) application (Tool Command Language (Tcl) or VoiceXML), use the **call application voice language** command in global configuration mode. To remove this language specification from the application, use the **no** form of this command.

call application voice *application-name* **language** *digit language*

no call application voice *application-name* **language** *digit language*

Syntax Description

application-name	Name of the application to which the language parameters are being passed.
digit	Number that identifies the language used by the audio files. Any number can represent any language. Enter 1 to indicate the primary language and 2 to indicate the secondary language. Range is from 0 to 9.
language	Two-character code that identifies the language of the associated audio files. Valid entries are as follows: • **en**—English • **sp**—Spanish • **ch**—Mandarin • **aa**—all

Command Default If this command is not configured, the default language is English.

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	This command was modified to support VoiceXML applications on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Release	Modification
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco 5800, and Cisco AS5850 in this release.
12.3(14)T	The **call application voice language** was replaced by the following commands: **param language** (application parameter configuration mode) **paramspace language** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command identifies the number that users enter for a language; for example, “Enter 1 for English. Enter 2 for French.”

This number is used only with the Tcl IVR Debit Card feature. Although it is not used by VoiceXML, you still must enter a number from 0 to 9.

Instead of using this command, you can configure the language and location of the prerecorded audio files within a Tcl script or VoiceXML document. For more information, see the *Tcl IVR API Version 2.0 Programmer’s Guide* or *Cisco VoiceXML Programmer’s Guide*, respectively.

To identify the location of the language audio files that are used for the dynamic prompts, use the **call application voice set-location** command.

Tcl scripts and VoiceXML documents can be stored in any of the following locations: On the TFTP, FTP, or HTTP servers, in the flash memory of the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations, and on RTSP servers.

With the Pre-Paid Debitcard Multi-Language feature, you can create Tcl scripts and a two-character code for any language. See the *Cisco Pre-Paid Debitcard Multi-Language Programmer's Reference*.

With the multilanguage support for Cisco IOS IVR, you can create a Tcl language module for any language and any set of TTS notations for use with Tcl and VoiceXML applications. See the *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response* document.

Table 3 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 3 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice language

        Warning: This command has been deprecated. Please use the following:
           param language
               paramspace language
```

The following example shows how to define the application "prepaid" and then selects English and Spanish as the languages of the audio files that are associated with the application:

```
call application voice prepaid tftp://keyer/debitcard.tcl
call application voice prepaid language 1 en
call application voice prepaid language 2 sp
```

Related Commands

Command	Description
call application voice	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Specifies the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param language	Configures the language parameter in a service or package on the gateway.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).
show call application voice	Displays information about voice applications.

call application voice load

To reload the selected voice application script after it has been modified, use the **call application voice load** command in privileged EXEC mode. This command does not have a **no** form.

call application voice load *application-name*

Syntax Description

application-name	Name of the Tcl or VoiceXML application to reload.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series (except for the Cisco 3660), and on the Cisco AS5300.
12.1(3)T	Support for dynamic script loading of Media Gateway Control Protocol (MGCP) was added.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(8)T	This command and implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and the Cisco AS5850 in this release.

Usage Guidelines

Use this command to reload an application Tcl script or VoiceXML document onto the gateway after it has been modified.

The location of the Tcl script or VoiceXML document for the specified application must have already been configured using the **call application voice** command.

Do not include the file type extension in the filename (.vxml or .tcl) when specifying the document used by the application.

Tcl scripts and VoiceXML documents can be stored in any of the following locations: on TFTP, FTP, or HTTP servers, in the flash memory of the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored on any of these locations, and on RTSP servers.

Before Cisco IOS Release 12.1(3)T, the software checked the signature in a Tcl script to ensure that it was supported by Cisco. A signature on Tcl scripts is no longer required. A signature has never been required for VoiceXML documents.

A Tcl script or VoiceXML document cannot be reloaded if it has active calls. Use the **show call application voice** command to verify that no active calls are using this application.

Tip If the **call application voice load** command fails to load the Tcl script or VoiceXML document that is associated with the application, enable the **debug voip ivr** command and retry. This debugging command can provide information on why loading fails.

Note MGCP scripting is not supported on the Cisco 1750 router or on Cisco 7200 series routers.

Examples

The following example shows the loading of a Tcl script called "clid_4digits_npw_3.tcl":

```
call application voice load clid_4digits_npw_3.tcl
```

The following example shows how to reload the VoiceXML application called "vapptest":

```
call application voice load vapptest
```

Related Commands

Command	Description
call application cache reload time	Configures the interval for reloading MGCP scripts.
call application voice	Creates and calls the application that interacts with the IVR feature.
debug http client	Displays information about the load an application that was loaded with HTTP.
show call application voice	Displays a list of the voice applications that are configured.

call application voice mail-script

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice mail-script** command is replaced by the **param mail-script** command in application parameter configuration mode. See the **param mail-script** command for more information.

To specify the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers, use the **call application voice mail-script** command in global configuration mode. To remove the application, use the **no** form of this command.

call application voice *mail-application-name* **mail-script** *application-name*

no call application voice *mail-application-name* **mail-script** *application-name*

Syntax Description

mail-application-name	Name of the off-ramp mail application that launches the app_voicemail_offramp.tcl script when the gateway receives an e-mail trigger.
application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(14)T	This command was replaced by the **param mail-script** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines To load the mail application onto the gateway, use the **call application voice** command.

The off-ramp mail application must be configured in the Multimedia Mail over Internet Protocol (MMoIP) dial peer that matches the telephone number contained in the header of the incoming e-mail message.

The off-ramp mail application must use the Tool Command Language (Tcl) script named "app_voicemail_offramp.tcl" that is provided by Cisco. This Tcl script can be downloaded from the Cisco website by following this path: Cisco > Technical Support Help - TAC > Select & Download Software > Software Center > Access Software > TclWare.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice mail-script

        Warning: This command has been deprecated. Please use the following:
           param mail-script
```

The following example shows that the off-ramp mail application named "offramp-mapp" hands calls to the application named "mapp-test" if the telephone number in the e-mail header is seven digits beginning with 555:

```
call application voice offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
call application voice mapp-test tftp://sample/tftp-users/vxml/user-test.vxml
call application voice offramp-mapp mail-script mapp-test
!
dial-peer voice 1001 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
application	Defines a specific voice application in the dial peer.
call application voice	Defines the name of a voice application and specifies the location of the document (Tcl or VoiceXML) to load for the application.
param mail-script	Specifies the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers.
show call application voice	Displays information about the configured voice applications.

call application voice mode

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice mode** command is replaced by the **param mode** command in application parameter configuration mode. See the **param mode** command for more information.

To direct the fax detection interactive voice response (IVR) application to operate in one of its four connection modes, use the **call application voice mode** command in global configuration mode. To return to the default connection mode, use the **no** form of this command.

call application voice *application-name* **mode** {**connect-first | listen-first | default-voice | default-fax**}

no call application voice *application-name* **mode** {**connect-first | listen-first | default-voice | default-fax**}

Syntax Description

application-name	Fax detection IVR application that was defined when the application was loaded on the router.
connect-first	Incoming calls are connected to the Real-Time Streaming Protocol (RTSP) server. This is the default.
listen-first	The gateway listens to the call first and then connects to the RTSP server. Any Dual tone multifrequency (DTMF) tones take the call to the voice server, but subsequent DTMF is forwarded as configured.
default-voice	Incoming calls are connected as voice calls to the RTSP server.
default-fax	Incoming calls are connected to the fax relay or store-and-forward fax application that is configured on the gateway.

Command Default **connect-first**

Command Modes Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco AS5300.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Release	Modification
12.3(14)T	This command was replaced by the **param mode** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

The call application voice mode commands control the way that the gateway handles fax detection IVR applications calls.

When the **connect-first** keyword is selected and CNG (calling) tones from the originating fax machine are detected, the voice application is disconnected and the call is passed to the configured fax application. If the **listen-first** keyword is selected, the gateway listens for CNG and, if it is detected, passes the call to the fax relay or store-and-forward fax application, whichever is configured on the gateway. When the **default-voice** and **default-fax** keywords are selected, the gateway defaults to voice after listening for CNG or passes the call to the fax relay or store-and-forward fax application, whichever was configured on the gateway. If the gateway hears the Dual tone multifrequency (DTMF) tones that are specified in the **call application voice voice-dtmf** or **call application voice fax-dtmf** commands, the call is forwarded as appropriate.

Note that in all four connection modes, the router continues to listen for CNG throughout the call, even if the call has been connected to the voice server; if CNG is detected, the call is connected to fax relay or store-and-forward fax, whichever has been configured.

This command is not supported by Cisco IOS help. If you type the **call application voice fax_detect mode** command and a question mark (?), Cisco IOS help does not supply a list of valid entries in place of the question mark.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice mode

        Warning: This command has been deprecated. Please use the following:
           param mode
```

The following example shows a selection of default-voice mode for the fax detection application:

```
call application voice fax_detect script_url
call application voice fax_detect mode default-voice
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice	Loads a specified IVR application onto the router from the TFTP server and gives it an application name by which it is known on the router.
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
call application voice fax-dtmf	Configures the fax detection IVR application to recognize a specified digit to indicate a fax call.

Command	Description
call application voice prompt	Configures the fax detection IVR application to use the specified audio file as a user prompt in listen-first mode, default-voice mode, or default-fax mode.
call application voice voice-dtmf	Configures the fax detection IVR application to recognize a specified digit to indicate a voice call.
param mode	Configures the call transfer mode for a package.

call application voice pin-len

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice pin-len** command is replaced with the **param pin-len** command in application parameter configuration mode. See the **param pin-len** command for more information.

To define the number of characters in the personal identification number (PIN) for the designated application, use the **call application voice pin-len** command in global configuration mode. To disable the PIN for the designated application, use the **no** form of this command.

call application voice *application-name* **pin-len** *number*

no call application voice *application-name* **pin-len** *number*

Syntax Description

application-name	Application name to which the PIN length parameter is being passed.
number	Number of allowable characters in PINs associated with the specified application. Range is from 0 to 10. The default is 4.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400 Cisco AS5800, and the Cisco AS5850 in this release.
12.3(14)T	The **call application voice pin-len** command was replaced with the **param pin-len** command in application parameter configuration mode.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a PIN for the specified application and to pass that information to the specified application.

Table 4 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 4 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4 **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice pin-len

        Warning: This command has been deprecated. Please use the following:
           param pin-len
```

The following example shows how to define a PIN length of 4 characters for the application named "prepaid":

```
call application voice prepaid pin-len 4
```

Related Commands

Command	Description
call application voice	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with the application.
call application voice language	Specifies the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice redirect-number	Specifies the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param pin-len	Defines the number of characters in the PIN for an application.

call application voice prompt

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice prompt** command is replaced by the **param prompt** command. See the **param prompt** command for more information.

To direct the fax detection interactive voice response (IVR) application to use the specified audio file as a user prompt, use the **call application voice prompt** command in global configuration mode. To disable use of this audio file, use the **no** form of this command.

call application voice *application-name* **prompt** *prompt-url*

no call application voice *application-name* **prompt** *prompt-url*

Syntax Description

application-name	Name of the fax detection IVR application that you defined when you loaded the application on the router.
prompt-url	URL or Cisco IOS file system location on the TFTP server for the audio file containing the prompt for the application.

Command Default

The prompt space is empty and no prompt is played.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced for the Cisco AS5300.
12.2(2)XB	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(14)T	This command was replaced by the **param prompt** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command is useful only in the listen-first, default-voice, and default-fax modes of the fax detection application.

Audio files should be a minimum of 9 seconds long so that callers do not hear silence during the initial CNG detection period. Any .au file can be used; formats are described in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

This command is not supported by Cisco IOS help. If you type the **call application voice fax_detect prompt** command with a question (?), the Cisco IOS help does not supply a list of entries that are valid in place of the question mark.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice prompt

        Warning: This command has been deprecated. Please use the following:
           param prompt
```

The following example associates the audio file" promptfile.au" with the application file "fax_detect", and the application with the inbound POTS dial peer:

```
call application voice fax_detect script_url
call application voice fax_detect mode default-voice
call application voice fax_detect prompt promptfile.au
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice	Loads a specified IVR application onto the router from the TFTP server and gives it an application name by which it is known on the router.
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
call application voice fax-dtmf	Configures the fax detection IVR application to recognize a specified digit to indicate a fax call.
call application voice mode	Configures the fax detection IVR application to operate in one of its four modes.
call application voice voice-dtmf	Configures the fax detection IVR application to recognize a specified digit to indicate a voice call.
param prompt	Directs the fax detection IVR application to use the specified audio file as a user prompt.

call application voice redirect-number

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice redirect-number** command is replaced with the **param redirect-number** command in application parameter configuration mode. See the the **param redirect-number** command for more information.

To define the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for the designated application, use the **call application voice redirect-number** command in global configuration mode. To cancel the redirect telephone number, use the **no** form of this command.

call application voice *application-name* **redirect-number** *number*

no call application voice *application-name* **redirect-number** *number*

Syntax Description

application-name	Name of the application to which the redirect telephone number parameter is being passed.
number	Designated operator telephone number of the service provider (or any other number designated by the customer). This is the number where calls are terminated when, for example, allowed debit time has run out or the debit amount is exceeded.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series, the Cisco 3600 series, and the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Release	Modification
12.3(14)T	This command was replaced by the **param redirect-number**.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the telephone number to which a call is redirected.

Table 5 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 5 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.

Table 5 Tcl Scripts and Commands (continued)

Tcl Script Name	Description	Commands to Configure
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice redirect-number

        Warning: This command has been deprecated. Please use the following:
           param redirect-number
```

The following example shows how to define a redirect number for the application named “prepaid”:

```
call application voice prepaid redirect-number 5550111
```

Related Commands

Command	Description
call application voice	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Specifies the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.

call application voice retry-count

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice retry-count** command is replaced by the **param retry-count** command in application parameter configuration mode. See the the **param retry-count** command for more information.

To define the number of times that a caller is permitted to reenter the personal identification number (PIN) for the designated application, use the **call application voice retry-count** command in global configuration mode. To cancel the retry count, use the **no** form of this command.

call application voice *application-name* **retry-count** *number*

no call application voice *application-name* **retry-count** *number*

Syntax Description

application-name	Name of the application to which the number of possible retries is being passed.
number	Number of times the caller is permitted to reenter PIN digits. Range is 1 to 5. The default is 3.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(4)T	This command was introduced on the Cisco 1750.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(14)T	This command was replaced by the **param retry-count** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define how many times a user can reenter a PIN.

Table 6 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 6 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application retry-count

        Warning: This command has been deprecated. Please use the following:
           param retry-count
```

The following example shows how to define that for the application named "prepaid" that a user can reenter a PIN three times before being disconnected:

```
call application voice prepaid retry-count 3
```

Related Commands

Command	Description
call application voice	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Specifies the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Specifies the telephone number to which a call is redirected for the designated application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param retry-count	Defines the number of times that a caller is permitted to reenter the PIN for a package.

call application voice security trusted

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice security trusted** command is replaced by the the following commands:

- **param security trusted** (application parameter configuration mode)
- **paramspace appcommon security trusted** (service configuration mode)

See these commands for more information.

To set the security level of a VoiceXML application to "trusted" so that automatic number identification (ANI) is not blocked, use the **call application voice security trusted** command in global configuration mode. To restore the default condition, use the **no** form of this command.

call application voice *application-name* **security trusted**

no call application voice *application-name* **security trusted**

Syntax Description

application-name	Name of the application being configured as trusted.

Command Default The security level of the application is not set to trusted, and ANI is blocked.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.
12.3(14)T	The **call application voice security trusted** command was replaced by the following commands: • **param security trusted** (application parameter configuration mode) • **paramspace appcommon security trusted** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines This command is applicable only for VoiceXML applications.

Note Tool Command Language (Tcl) applications provide the security parameter to the application but do not use it.

If an application is configured as a trusted application, it is trusted not to provide the calling number to the destination party, so ANI is always provided if available.

Normally, the voice gateway does not provide the calling number (ANI) to a VoiceXML application if the caller ID is blocked. Caller ID is blocked if a call that comes into the voice gateway has the presentation indication field set to "presentation restricted". The session.telephone.ani variable is set to "blocked". When the **call application voice security trusted** command is configured, the gateway does not block caller ID; it provides the calling number to the VoiceXML application.

If the keyword of this command is set to anything other than **trusted**, the value is accepted and the application is treated as not trusted. For example, in the following configuration, the application "sample" is treated as not trusted, and caller ID is blocked:

```
call application voice sample security not_trusted
```

To enable Generic Transparency Descriptor (GTD) parameters in call signaling messages to map to VoiceXML and Tcl session variables, configure the **call application voice security trusted** command. If this command is not configured, the VoiceXML variables that correspond to GTD parameters are marked as not available. For a detailed description of the VoiceXML and Tcl session variables, see the *Cisco VoiceXML Programmer's Guide* and the *Tcl IVR API Version 2.0 Programmer's Guide*, respectively.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice security trusted

        Warning: This command has been deprecated. Please use the following:
           param security trusted (application parameter configuration mode)
               paramspace appcommon security trusted
```

The following example configures the application "sample" as a trusted application. Caller ID is available to this VoiceXML application if it is supported by the service provider.

```
call application voice sample flash:sample.vxml
call application voice sample security trusted
```

The following example configures the application "example" as not trusted. Caller ID can be blocked.

```
call application voice coldcall tftp://joeserver/sellcars.vxml
no call application voice example security trusted
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specifies the location of the document (Tcl or VoiceXML) to load for the application.
call application voice language	Defines the language of the audio files used for dynamic prompts by the designated application.
call application voice load	Reloads a Tcl or VoiceXML document.
call application voice pin-len	Defines the number of characters in the PIN for the Tcl application.
call application voice redirect-number	Defines the telephone number to which a call is redirected for the designated application.

Command	Description
call application voice retry-count	Defines the number of times that a caller is permitted to reenter the PIN for a designated application.
call application voice uid-len	Defines the number of characters in the UID for the designated application.
call application voice warning-time	Defines the number of seconds for which a warning prompt is played before a user's account time runs out.
param security	Configures security for linkable Tcl functions (packages).
paramspace appcommon security	Configures security for a service (application).
show call application voice	Displays the following information associated with a voice application: the audio files, the prompts, the caller interaction, and the abort key operation.

call application voice set-location

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice set-location** command is replaced by the **paramspace language** command. See the **paramspace language** command for more information.

To define the category and location of audio files that are used for dynamic prompts by the specified IVR application (Tcl or VoiceXML), use the **call application voice set-location** command in global configuration mode. To remove these definitions, use the **no** form of this command.

call application voice *application-name* **set-location** *language category location*

no call application voice *application-name* **set-location** *language category location*

Syntax Description

application-name	Name of the application to which the **set-location** parameters are being passed.
language	Two-character code that identifies the language associated with the audio files. Valid entries are as follows: • **en**—English • **sp**—Spanish • **ch**—Mandarin • **aa**—All This is the same language code that was entered when configuring the **call application voice language** command .
category	Category group of the audio files (from 0 to 4). For example, audio files representing the days and months can be category 1, audio files representing units of currency can be category 2, and audio files representing units of time—seconds, minutes, and hours—can be category 3. Range is from 0 to 4; 0 means all categories.
location	URL of the audio files. Valid URLs refer to TFTP, FTP, HTTP, or RTSP servers, flash memory, or the removable disks on the Cisco 3600 series.

Command Default No location or category is set.

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(2)XB	This command was modified to support VoiceXML applications on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(14)T	This command was replaced by the **paramspace language** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Instead of using this command, you can configure the language and location of prerecorded audio files within a Tcl script or VoiceXML document. For more information, see the *Tcl IVR API Version 2.0 Programmer's Guide* or *Cisco VoiceXML Programmer's Guide*, respectively.

To identify the language of the audio files, use the **call application voice language** command.

Tcl scripts and VoiceXML documents can be stored in any of the following locations: On TFTP, FTP, or HTTP servers, in the flash memory on the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations, and on RTSP servers.

You can configure multiple set-location lines for a single application.

With the Pre-Paid Debitcard Multi-Language feature, you can create Tcl scripts and a two-character code for any language. See the *Cisco Pre-Paid Debitcard Multi-Language Programmer's Reference*.

With the multilanguage support for Cisco IOS IVR, you can create a Tcl language module for any language and any set of Text-to-Speech (TTS) notations for use with Tcl and VoiceXML applications. See the *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response* document.

Table 7 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 7 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None

Table 7 Tcl Scripts and Commands (continued)

Tcl Script Name	Description	Commands to Configure
clid_4digits_npw_3_cli.tcl	Authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	Authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	Authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	Authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	Authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice set-location

        Warning: This command has been deprecated. Please use the following:
           paramspace language
```

The following example shows how to configure the **call application voice set-location** command for the application named "prepaid." In this example, the language specified is English, the category into which the audio files are grouped is category 0 (meaning all), and the location is the keyer directory on the TFTP server.

```
call application voice prepaid set-location en 0 tftp://keyer/
```

The following example shows how to configure the **call application voice set-location** command for a fictitious VoiceXML application named "sample." In this example, as in the preceding example, the language defined is English, the category into which the audio files are grouped is category 0 (meaning "all") and the location is the example directory on an HTTP server.

```
call application voice sample set-location en 0 http://example/
```

The following example shows how to configure the **call application voice set-location** command for multiple set locations:

```
call application voice sample set-location en 0 http://example/en_msg/
call application voice sample set-location sp 0 http://example/sp_msg/
call application voice sample set-location ch 0 http://example/ch_msg/
```

Related Commands

Command	Description
call application voice	Specifies the application name and indicates the location of the IVR script to be used with this application.
call application voice language	Specifies the audio file language for the designated application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Specifies the number of characters in the PIN.
call application voice redirect-number	Specifies the telephone number to which a call is redirected.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN.
call application voice uid-len	Defines the number of characters in the UID for the designated application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).
show call application voice	Displays information about voice applications.

call application voice transfer mode

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice transfer mode** command is replaced by the following commands:

- **param mode** (application parameter configuration mode)
- **paramspace callsetup mode** (service configuration mode)

See these commands for more information.

To specify the call-transfer method for Tool Command Language (Tcl) or VoiceXML applications, use the **call application voice transfer mode** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application voice *application-name* **transfer mode** {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}

no call application voice *application-name* **transfer mode**

Syntax Description

application-name	Name of the voice application for which the transfer method is set.
redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Provides support for Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Provides support for TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as for the **redirect-at-connect** keyword.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default Rotary method; call redirection is not invoked.

Command Modes Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(14)T	This command was replaced by the following commands: • **param mode** (application parameter configuration mode) • **paramspace callsetup mode** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command determines whether a voice application can invoke TBCT or RTPvt. Before you can use this command, you must configure the named application on the gateway by using the **call application voice** command.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected if the call leg is capable of it.

Tcl scripts can read the value of this command by using the info tag get cfg_avpair transfer-mode statement. For detailed information, see the *Tcl IVR API Version 2.0 Programmer's Guide*.

For VoiceXML applications, the value of this command becomes the default behavior if the com.cisco.transfer.mode property is not specified in the VoiceXML document. For detailed information, see the *Cisco VoiceXML Programmer's Guide*. The VoiceXML document property takes precedence over the gateway configuration.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice transfer mode

        Warning: This command has been deprecated. Please use the following:
           param mode
               paramspace callsetup mode
```

The following example sets the transfer method to redirect for the application callme:

```
call application voice callme transfer mode redirect
```

Related Commands

Command	Description
application	Enables a voice application on a dial peer.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.
call application voice transfer reroute-mode	Specifies the call-forwarding behavior of a Tcl application.
debug voip ivr callsetup redirect	Displays debugging information about H.450 calls that are redirected during setup.
debug voip ivr redirect	Displays debugging information about redirected H.450 calls.
isdn supp-service tbct	Enables ISDN TBCT on PRI trunks.
param mode	Configures the call transfer mode for a package.

Command	Description
paramspace callsetup mode	Configures the call transfer mode for an application.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
show call application voice	Displays information about voice applications.
show call history voice redirect	Displays history information about calls that were redirected using RTPvt or TBCT.

call application voice transfer reroute-mode

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice transfer reroute-mode** command is replaced by the following commands:

- **param reroutemode** (application parameter configuration mode)
- **paramspace callsetup reroutemode** (service configuration mode)

See these commands for more information.

To specify the call-forwarding behavior of a Tool Command Language (Tcl) application, use the **call application voice transfer reroute-mode** command in global configuration mode. To reset to the default, use the **no** form of this command.

call application voice *application-name* **transfer reroute-mode** {**none** | **redirect** | **redirect-rotary** | **rotary**}

no call application voice *application-name* **transfer reroute-mode**

Syntax Description

application-name	Name of the voice application for which the transfer reroute method is set.
none	Call forwarding is not performed by the voice application.
redirect	Two call legs are directly connected. Provides support for RTPvt.
redirect-rotary	Two call legs are directly connected (redirect). If that fails, the two call legs are hairpinned on the gateway (rotary).
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two calls together. RTPvt is not invoked. This is the default.

Command Default

Rotary method; RTPvt is not invoked.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(14)T	This command was replaced by the following commands: • **param reroutemode** (application parameter configuration mode) • **paramspace callsetup reroutemode** (service configuration mode)
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Before you can use this command, you must configure the named application on the gateway by using the **call application voice** command. This command is not supported for VoiceXML applications or for TBCT.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected, provided that the call leg is capable of it.

Tcl scripts can read the value of this command by using the info tag get cfg_avpair reroute-mode statement. For detailed information, see the *Tcl IVR API Version 2.0 Programmer's Guide*.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice transfer reroute-mode

        Warning: This command has been deprecated. Please use the following:
           param reroutemode (application parameter configuration mode)
               paramspace callsetup reroutemode
```

The following example sets the call forwarding method to redirect for the application callme:

```
call application voice callme transfer reroute-mode redirect
```

Related Commands

Command	Description
application	Enables a voice application on a dial peer.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.
call application voice transfer mode	Specifies the call-transfer behavior of a Tcl or VoiceXML application.
isdn supp-service tbct	Enables ISDN TBCT on PRI trunks.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
show call application voice	Displays information about voice applications.
show call history voice redirect	Displays history information about calls that were redirected using RTPvt or TBCT.

call application voice uid-length

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice uid-length** command is replaced by the **param uid-len** command. See the **param uid-len** command for more information.

To define the number of characters in the user identification (UID) number for the designated application and to pass that information to the specified application, use the **call application voice uid-length** command in global configuration mode. To restore the default setting for this command, use the **no** form of this command.

call application voice *application-name* **uid-length** *number*

no call application voice *application-name* **uid-length** *number*

Syntax Description

application-name	Name of the application to which the UID length parameter is passed.
number	Number of allowable characters in UIDs that are associated with the specified application. Range is from 1 to 20. The default is 10.

Command Default

number

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751. This release does not support any other Cisco platforms.
12.2(4)T	Support was added for the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(14)T	This command was replaced by the **param uid-len** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a UID for the specified application and to pass that information to the specified application.

Table 8 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 8 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	Authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	Authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	Authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	Authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	Authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice uid-length

        Warning: This command has been deprecated. Please use the following:
           param uid-len
```

The following example shows how to configure four allowable characters in the UID for the application named “sample”:

```
call application voice sample uid-length 4
```

Related Commands

Command	Description
call application voice	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Specifies the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Specifies the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice warning-time	Defines, in seconds, how long in advance a user is warned before the allowed calling time expires for the designated application.
param uid-length	Defines the number of characters in the UID for a package.

call application voice voice-dtmf

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice voice-dtmf** command is replaced by the **param voice-dtmf** command. See the **param voice-dtmf** command for more information.

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a voice call, use the **call application voice voice-dtmf** command in global configuration mode. To remove configuration of this digit, use the **no** form of this command.

call application voice *application-name* **voice-dtmf** {*keypad-character*}

no call application voice *application-name* **voice-dtmf** {*keypad-character*}

Syntax Description

application-name	The name of the fax detection application that you defined when you loaded the application on the router.
keypad-character	Single character that can be dialed on a telephone keypad pressed by the calling party to indicate a voice call, in response to the audio prompt configured in default-voice and default-fax mode of the fax detection IVR application. Default is 1.

Command Default

1

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced for the Cisco AS5300.
12.2(2)XB	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.3(14)T	This command was replaced by the **param voice-dtmf** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode, as defined by the **call application voice mode** command. Only one digit can be specified in this command, and that digit must be different from the digit specified in the **call**

application voice fax-dtmf command. You are not notified immediately if you make the error of configuring them both to the same digit. To find this error, you must start debugging with the **debug voip ivr script** command and then observe some failing calls.

This command is not supported by Cisco IOS help. If you type **the call application voice fax_detect voice-dtmf** command and a question mark (**?**), the Cisco IOS help does not supply a list of entries that are valid in place of the question mark.

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice voice-dtmf

        Warning: This command has been deprecated. Please use the following:
           param voice-dtmf
```

The following example selects digit 2 dual tone multifrequency (DTMF) to indicate a voice call:

```
call application voice fax_detect script_url
call application voice fax_detect voice-dtmf 2
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice	Loads a specified IVR application onto the router from the TFTP server and gives it an application name by which it is known on the router.
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
call application voice fax-dtmf	Configures the fax detection IVR application to recognize a specified digit to indicate a fax call.
call application voice mode	Configures the fax detection IVR application to operate in one of its four modes.
call application voice prompt	Configures the fax detection IVR application to use the specified audio file as a user prompt.
param voice-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a voice call.

call application voice warning-time

Note Effective with Cisco IOS Release 12.3(14)T, the **call application voice warning-time** command is replaced by the **param warning-time** command. See the **param warning-time** command for more information.

To define the number of seconds of warning that a user receives before the allowed calling time expires use the **call application voice warning-time** command in global configuration mode. To remove the configured warning period, use the **no** form of this command.

call application voice *application-name* **warning-time** *seconds*

no call application voice *application-name* **warning-time** *seconds*

Syntax Description

application-name	Name of the application to which the warning time parameter is being passed.
seconds	Length of the warning period, in seconds, before the allowed calling time expires. Range is from 10 to 600. This argument has no default value.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1751. Support for other Cisco platforms is not included in this release.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(14)T	This command was replaced by the **param warning-time** command.
12.4(24)T	This command was modified. The automatic conversion to the new CLI is replaced with an explicit error message.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of seconds in the warning period before the allowed calling time expires for the specified application and to pass that information to the specified application.

Table 9 lists Tcl script names and the corresponding commands that are required for each Tcl script.

Table 9 Tcl Scripts and Commands

Tcl Script Name	Description	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and personal identification number (PIN) using the following: prompt-user, using automatic number identification (ANI), dialed number identification service (DNIS), gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. The number of digits allowed for the account number and password, respectively, are configurable through the command-line interface (CLI). If the authentication fails, the script allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-length** Range is 1 to 20. The default is 10. **call application voice pin-length** Range is 0 to 10. The default is 4. **call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN, respectively, using ANI and NULL. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, the script allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_3_cli.tcl	This script authenticates using ANI and NULL for account numbers and PINs, respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** Range is 1 to 5. The default is 3.
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and NULL for account and PIN, respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	**call application voice retry-count** Range is 1 to 5. The default is 3.
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Examples

Effective with Cisco IOS Release 12.4(24)T, the following warning message is displayed to direct users to the replacement command options:

```
Router(config)# call application voice param warning-time

        Warning: This command has been deprecated. Please use the following:
           param warning-time
```

The following example shows how to configure a 30-second warning time for the application named "sample":

```
call application voice sample warning-time 30
```

Related Commands

Command	Description
call application voice language	Specifies the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reloads the designated Tcl script.
call application voice location	Specifies the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Specifies the telephone number to which a call is redirected for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-length	Defines the number of characters in the UID for the designated application and passes that information to the application.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

call-block (dial peer)

To enable blocking of incoming calls, use the **call-block** command in dial peer configuration mode. To return to the default value, use the **no** form of this command.

call-block {**disconnect-cause incoming** {**call-reject** | **invalid-number** | **unassigned-number** | **user-busy**} | **translation-profile incoming** *name*}

no call-block {**disconnect-cause incoming** {**call-reject** | **invalid-number** | **unassigned-number** | **user-busy**} | **translation-profile incoming** *name*}

Syntax Description

disconnect-cause incoming	Associates a disconnect cause of incoming calls.
call-reject	Specifies call rejection as the cause for blocking a call during incoming call-number translation.
invalid-number	Specifies invalid number as the cause for blocking a call during incoming call-number translation.
unassigned-number	Specifies unassigned number as the cause for blocking a call during incoming call-number translation.
user-busy	Specifies busy as the cause for blocking a call during incoming call-number translation.
translation-profile incoming	Associates the translation profile for incoming calls.
name	Name of the translation profile.

Command Default

Disconnect cause: No Service (once the call-blocking translation profile is defined)
Translation profile: No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

An incoming call can be blocked from the gateway if one of the call numbers (calling, called, or redirect) is matched with the reject translation rule of the incoming call-blocking translation profile.

The cause value is returned to the source of the call when a call is blocked during the incoming call-number translation.

This command is supported in POTS, VoIP, VoFR, and VoATM dial-peer configuration. For VoATM, only ATM Adaptation Layer 5 (AAL5) calls are supported.

The only option for call blocking is in the incoming direction. From the perspective of the voice gateway, the incoming direction can be either of the following:

- Incoming from a telephony device directly attached to a voice port on the gateway toward the gateway itself
- Incoming by way of an inbound Voice over X (VoX) call from a peer gateway

To configure incoming call blocking, define a translation rule with a **reject** keyword. For example:

```
voice translation-rule 1
 rule 1 reject /408252*/
```

Apply the rule to a translation profile for called, calling, or redirect-called numbers, such as:

```
voice translation profile call_block_profile
 translate calling 1
```

Include the translation profile within a dial peer definition. For example:

```
dial-peer voice 111 pots
 call-block translation-profile incoming call_block_profile
 call-block disconnect-cause incoming invalid_number
```

In this example, the gateway blocks any incoming time-division multiplexing (TDM) call that successfully matches inbound dial-peer 111 and has a calling number that starts with 408252. The gateway also returns the disconnect cause “invalid number” to the source of the call. (Other disconnect causes can be assigned: unassigned-number, user-busy, or call-rejected.)

Examples

The following example assigns the translation profile “example” to be used for incoming calls and returns the message “invalid number” as a cause for blocked calls:

```
Router(config)# dial-peer voice 5 pots
Router(config-dial-peer)# call-block translation-profile incoming example
Router(config-dial-peer)# call-block disconnect-cause incoming invalid-number
```

Following are two possible call-blocking scenarios:

Scenario 1: Block Inbound Calls from the PSTN/PBX/CO

We place the rejection profile on a POTS dial peer that is associated with the voice port on which we expect the inbound call. When the inbound call attempt is made, we see in the CCAPI debugs that POTS dial-peer 9 is matched for the telephony call leg. The call-block rule is checked and we send back user-busy to the switch.

```
voice translation-rule 1
 rule 1 reject /9193927582/   <<<<-------- filter out calls from this CallerID

voice translation-profile reject_ANI
 translate calling 1

dial-peer voice 9 pots
 destination-pattern 9T
 direct-inward-dial
 port 1/0:23
 call-block translation-profile incoming reject_ANI
 call-block disconnect-cause incoming user-busy
```

Scenario 2: Block Inbound VoX Calls from Using Local POTS Resources

We place the rejection profile on a VoIP/VoATM/VoFR dial peer that matches an inbound VoX call attempt. When the inbound call attempt is made, we see in the CCAPI debugs that VoIP dial-peer 7 is matched for the IP call leg. The call-block rule is checked and we send back user-busy to the switch.

```
voice translation-rule 1
 rule 1 reject /9193927582/   <<<<-------- filter out calls from this CallerID

voice translation-profile reject_ANI
 translate calling 1

dial-peer voice 7 voip
 destination-pattern 7T
 session target ipv4:A.B.C.D
 incoming called-number .   <<<<-------- force inbound IP call-leg match
 call-block translation-profile incoming reject_ANI
 call-block disconnect-cause incoming user-busy
```

Related Commands

Command	Description
dial-peer voice	Initiates the dial-peer voice configuration mode.
voice translation-profile	Defines a translation profile for voice calls.
voice translation-rule	Defines a translation rule for voice calls.

call-denial

The **call-denial** command is replaced by the **call threshold global** command. See the **call threshold global** command for more information.

call fallback

To enable a call request to fall back to a specific dial peer in case of network congestion, use the **call fallback** command in dial peer configuration mode. To disable PSTN fallback for a specific dial peer, use the **no** form of this command.

call fallback

no call fallback

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default if the **call fallback active** command is enabled in global configuration mode

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Disabling the **call fallback** command for a dial peer causes the call fallback subsystem not to fall back to the specified dial peer. Disabling the command is useful when internetworking fallback capable H.323 gateways with the Cisco CallManager or third-party equipment that does not run fallback. Connected calls are not affected by this feature.

Examples

The following example disables a PSTN fallback for a specific dial peer:

```
no call fallback
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers.
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Configures the call fallback subsystem to take an average from the last two cache entries for call requests.

Command	Description
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.
show call fallback config	Displays the call fallback configuration.

call fallback active

To enable the Internet Control Message Protocol (ICMP)-ping or Service Assurance Agent (SAA) (formerly Response Time Reporter [RTR]) probe mechanism for use with the dial-peer **monitor probe** or voice-port **busyout monitor probe** commands, use the **call fallback active** command in global configuration mode. To disable these probe mechanisms, use the **no** form of this command.

call fallback active [**icmp-ping** | **rtr**]

no call fallback active [**icmp-ping** | **rtr**]

Syntax Description

icmp-ping	Uses ICMP pings to monitor the IP destinations.
rtr	Uses SAA (formerly RTR) probes to monitor the IP destinations. SAA (RTR) probes are the default.

Command Default

This command is disabled by default. If the command is entered without an optional keyword, the default is RTR.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented for Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **call fallback active** command creates and maintains a consolidated cache of probe results for use by the dial-peer **monitor probe** or voice-port **busyout monitor probe** commands.

Enabling the **call fallback active** command determines whether calls should be accepted or rejected on the basis of probing of network conditions. The **call fallback active** command checks each call request and rejects the call if the network congestion parameters are greater than the value of the configured threshold parameters of the destination. If this is the case, alternative dial peers are tried from the session application layer.

Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.

Connected calls are not affected by this command.

Caution The **call fallback active icmp-ping** command must be entered before the **call fallback icmp-ping** command can be used. If you do not enter this command first, the **call fallback icmp ping** command will not work properly.

Note The Cisco SAA functionality in Cisco IOS software was formerly known as Response Time Reporter (RTR). The command-line interface still uses the keyword **rtr** for configuring RTR probes, which are now actually SAA probes.

Examples

The following example enables the **call fallback active** command and globally enables ICMP pinging to probe target destinations. The second command specifies values for the ping packets:

```
Router(config)# call fallback active icmp-ping
Router(config)# call fallback icmp-ping codec g729 interval 10 loss 10
```

Related Commands

Command	Description
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Specifies the call fallback subsystem to take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.

call fallback cache-size

To specify the call fallback cache size for network traffic probe entries, use the **call fallback cache-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback cache-size *number*

no call fallback cache-size

Syntax Description

number	Cache size, in number of entries. Range is from 1 to 256. The default is 128.

Command Default

128 entries

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced..
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The cache size can be changed only when the **call fallback active** command is not enabled.

The overflow process deletes up to one-fourth of the cache entries to allow for additional calls beyond the specified cache size. The cache entries chosen for deletion are the oldest entries in the cache.

If the cache size is left unchanged, it can be changed only when fallback is off. Use the **no** form of the **call fallback** command to turn fallback off.

Examples

The following example specifies 120 cache entries:

```
Router(config)# call fallback cache-size 120
```

Related Commands

Command	Description
call fallback	Enables a call request to fall back to a specific dial peer in case of network congestion
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.

Command	Description
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.
show call fallback config	Displays the call fallback configuration.

call fallback cache-timeout

To specify the time after which the cache entries of network conditions are purged, use the **call fallback cache-timeout** command in global configuration mode. To disable the **call fallback cache-timeout** command, use the **no** form of this command.

call fallback cache-timeout *seconds*

no call fallback cache-timeout

Syntax Description

seconds	Cache timeout value, in seconds. Range is from 1 to 2147483. The default is 600.

Command Default

600 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Enabling the **call fallback cache-timeout** command sends a Service Assurance Agent (SAA) probe out to the network to determine the amount of congestion in terms of configured thresholds. The network condition is based upon delay and loss, or Calculated Planning Impairment Factor (ICPIF) thresholds. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.

The cache keeps entries for every network congestion-checking probe sent and received between timeouts. The cache updates after each probe returns the current condition of network traffic. To set the probe frequency, use the **call fallback probe-timeout** command.

When a call comes into the router, the router matches a dial peer and obtains the destination information. The router calls the fallback subsystem to look up the specified destination in its network traffic cache. If the delay/loss or ICPIF threshold exists and is current, the router uses that value to decide whether to permit the call into the Voice over IP (VoIP) network. If the router determines that the network congestion is below the configured threshold (by looking at the value in the cache), the call is connected.

After each call request, the timer is reset. Purging of the cache occurs only when the cache has received no call requests during the timeout period (*seconds*). When the cache timeout expires, the entire cache is deleted, and a probe is sent to start a new cache entry. A call cannot be completed until this probe returns with network traffic information.

The network congestion probes continue in the background as long as the entry for the last call request remains in the cache.

Examples

The following example specifies an elapsed time of 1200 seconds before the cache times out:

```
Router(config)# call fallback cache-timeout 1200
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback cache-size	Specifies the call fallback cache size.
call fallback probe-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback threshold delay loss	Configures the call fallback threshold to use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.
show call fallback config	Displays the call fallback configuration.

call fallback expect-factor

To set a configurable value by which the call fallback expect factor feature will be activated, use the **call fallback expect-factor** command in global configuration mode. To disable the expect factor, use the **no** form of this command.

call fallback expect-factor *value*

no call fallback expect-factor

Syntax Description

value	Configures the expect-factor A. Range: 0 to 20. Default: 10.

Command Default No value for the expect-factor is configured.

Command Modes Global configuration

Command History

Release	Modification
12.3(3)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The expect-factor is the level of expected voice quality that the user may have during a call. For example, you expect higher voice quality from a call on your home than on your cell phone. The expect-factor is a subjective value determined by the local administrators.

Call fallback is used by the software to generate a series of probes across an IP network to help make a Impairment/Calculated Impairment Planning Factor (ICPIF) calculation. The value calculated by the probes, ICPIF, is modified by the configured expect factor using the following formula:

ICPIF = Idd + Ie–A

Idd represents the impairment due to end-end delay, Ie, represents the impairment due to packet loss and the impact of the codec being used on the call, and A represents the expect-factor value. The expect-factor is the value to be subtracted from the calculated ICPIF value. This expect factor is known as the Advantage Factor (A) as specified in G.107 and takes into account the user's expected level of voice quality based upon the type of call being made.

Examples The following example shows the **call fallback expect-factor** command and the **call fallback threshold icpicf** command being configured. A calculated ICPIF value of 20 based on Idd and Ie from the probes set on a IP network would not activate the call fallback feature in this configuration. Even though the calculated ICPIF value of 20 exceeds the configured threshold of 10, subtraction of the expect-value of 15 would leave a value of 5, which is below the threshold value.

```
Router(config)# call fallback expect-factor 15
Router(config)# call fallback threshold icpif 10
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers.
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Configures the call fallback subsystem to take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies use of MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
dial-peer voice number	Enters dial peer configuration mode.
show call fallback config	Displays the call fallback configuration.

call fallback icmp-ping

To specify Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations and configure parameters for the ping packets, use the **call fallback icmp-ping** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback icmp-ping [**count** *packets*] [**codec** *codec-type* | **size** *bytes*] **interval** *seconds* [**loss** *percent]* **timeout** *milliseconds*]

no call fallback icmp-ping [**count** *packets*] [**codec** *codec-type* | **size** *bytes*] **interval** *seconds* [**loss** *percent]* **timeout** *milliseconds*]

Syntax Description

count *packets*	(Optional) Number of ping packets that are sent to the destination address.
codec	(Optional) Configures the profile of the SAA probe signal to mimic the packet size and interval of a specific codec type.
codec-type	(Optional) The codec type for the SAA probe signal. Available options are as follows: • **g711a**—G.711 a-law • **g711u**—G.711 mu-law • **g729**—G.729 (the default) • **g729b**—G.729 Annex B
size *bytes*	(Optional) Size (in bytes) of the ping packet. Default is 32.
interval *seconds*	Time (in seconds) between ping packet sets. Default is 5. This number should be higher than the **timeout** *milliseconds* value.
loss *percent*	(Optional) Configures the percentage-of-packets-lost threshold for initiating a busyout condition.
timeout *milliseconds*	(Optional) Timeout (in milliseconds) for echo packets. Default is 500.

Command Default

If this command is not configured, Response Time Reporter (RTR) is the probe method used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(2)T.

Usage Guidelines

The values configured by the global configuration version of the **call fallback icmp-ping** command are appllied globally for measurements on probes and pings. If the **call fallback icmp-ping** is configured in dial-peer configuration mode, these values override the global configuration for the specific dial peer.

One of these two commands must be in effect before the **monitor probe icmp-ping** command can be used. If neither of the **call fallback** commands is in effect, the **monitor probe icmp-ping** command will not work properly.

Examples

The following example shows how to configure an ICMP ping probe with a G.729 profile to probe the link with an interval value of 10 seconds and a packet-loss threshold of 10 percent:

```
call fallback active icmp-ping
call fallback icmp-ping codec g729 interval 10 loss 10
```

Related Commands

Command	Description
call fallback active	Forces a voice port into the busyout state.
call fallback icmp-ping (dial peer)	Specifies Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations.
monitor probe icmp-ping	Enables dial-peer status changes based on the results of probes.

call fallback icmp-ping (dial peer)

To specify Internet Control Message Protocol (ICMP) ping as the method for network traffic probe entries to IP destinations, use the **call fallback icmp-ping** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

call fallback [**icmp-ping** | **rtr**]

no call fallback [**icmp-ping** | **rtr**]

Syntax Description

icmp-ping	(Optional) Specifies ICMP ping as the method for monitoring the session target and updating the status of the dial peer.
rtr	(Optional) Specifies that the Response Time Reporter (RTR) probe is the method for monitoring the session target and updating the status of the dial peer.

Command Default

If this command is not entered, the globally configured method is used for measurements.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.

Usage Guidelines

The principal use of this command is to specify ICMP ping as the probe method, even though the option for selecting RTR is also available.

If the **call fallback icmp-ping** command is not entered, the **call fallback active** command in global configuration is used for measurements. If the **call fallback icmp-ping** command is entered, these values override the global configuration.

One of these two commands must be in effect before the **monitor probe icmp-ping** command can be used. If neither of the **call fallback** commands is in effect, the **monitor probe icmp-ping** command will not work properly.

Note The Cisco Service Assurance Agent (SAA) functionality in Cisco IOS software was formerly known as Response Time Reporter (RTR). The command-line interface still uses the keyword **rtr** for configuring RTR probes, which are now actually the SAA probes.

Examples

The following example specifies that ICMP ping is used for monitoring the session target IP address and for updating the status of the dial peer:

```
Router(config)# dial-peer voice 10 voip
Router(config-dial-peer)# call fallback icmp-ping
```

Related Commands

Command	Description
call fallback	Enables a call request to fall back to a specific dial peer in case of network congestion
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
monitor probe icmp-ping	Specifies that ICMP ping is the method used for probes.
show call fallback config	Displays the call fallback configuration.

call fallback instantaneous-value-weight

To configure the call fallback subsystem to take an average from the last two probes registered in the cache for call requests, use the **call fallback instantaneous-value-weight** command in global configuration mode. To return to the default before the average was calculated, use the **no** form of this command.

call fallback instantaneous-value-weight *percent*

no call fallback instantaneous-value-weight

Syntax Description

percent	Instantaneous value weight, in expressed as a percentage. Range is from 0 to 100. The default is 66.

Command Default 66 percent

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines Probes that return the network congestion information are logged into the cache to determine whether the next call request is granted. When the network is regularly busy, the cache entries reflect the heavy traffic conditions. However, one probe may return with low traffic conditions, which is in contrast to normal conditions. All call requests received between the time of this probe and the next use this entry to determine call acceptance. These calls are allowed through the network, but before the next probe is sent and received, the normal, heavy traffic conditions must have returned. The calls sent through congest the network and cause worsen traffic conditions.

Use the **call fallback instantaneous-value-weight** command to gradually recover from heavy traffic network conditions. While the system waits for a call, probes update the cache. When a new probe is received, the *percentage* is set and indicates how much the system is to rely upon the new probe and the previous cache entry. If the *percentage* is set to 50 percent, the system enters a cache entry based upon an average from the new probe and the most recent entry in the cache. Call requests use this blended entry to determine acceptance. This allows the call fallback subsystem to keep conservative measures of network congestion.

The configured *percentate* applies to the new probe first. If the **call fallback instantaneous-value-weight** command is configured with the default *percentage* of 66 percent, the new probe is given a higher value to calculate the average for the new cache entry.

Examples

The following example specifies a fallback value weight of 50 percent:

```
Router(config)# call fallback instantaneous-value-weight 50
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
show call fallback config	Displays the call fallback configuration.

call fallback jitter-probe dscp

To specify the differentiated services code point (DSCP) of the jitter-probe transmission, use the **call fallback jitter-probe dscp** command in global configuration mode. To disable this feature and restore the default value of jitter-probe precedence, use the **no** form of this command.

call fallback jitter-probe dscp *dscp-number*

no call fallback jitter-probe dscp

Syntax Description

dscp-number	DSCP value. Range is from 0 to 63.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(9)	This command was implemented in Cisco IOS Release 12.3(9).

Usage Guidelines

Network devices that support differentiated services (DiffServ) use a DSCP in the IP header to select a per-hop behavior (PHB) for a packet. Cisco implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. On the basic of DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated alike.

The **call fallback jitter-probe dscp** command allows you to set a DSCP for jitter-probe packets. The specified DSCP is stored, displayed, and passed in probing packets to the Service Assurance Agent (SAA). This command enables the router to reserve some bandwidth so that during network congestion some of the jitter-probe packets do not get dropped. This command avoids the conflict that occurs with traditional precedence bits.

The **call fallback jitter-probe dscp** command is mutually exclusive with the **call fallback jitter-probe precedence** command. Only one of these command can be enabled on the router. When the **call fallback jitter-probe dscp** command is configured, the precedence value is replaced with the DSCP value. The **no call fallback jitter-probe dscp** command restores the default value for precedence.

Examples

The following example specifies the jitter-probe DSCP as 10. DSCP configuration replaces the set jitter-probe precedence value with the DSCP value.

```
call fallback jitter-probe dscp 10
```

The following configuration disables the DSCP value and restores the default value for precedence, which is set to 2:

```
no call fallback jitter-probe dscp
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
show call fallback config	Displays the call fallback configuration.

call fallback jitter-probe num-packets

To specify the number of packets in a jitter probe used to determine network conditions, use the **call fallback jitter-probe num-packets** command in global configuration mode. To restore the default number of packets, use the **no** form of this command.

call fallback jitter-probe num-packets *number-of-packets*

no call fallback jitter-probe num-packets

Syntax Description

number-of-packets	Number of packets. Range is from 2 to 50. The default is 15.

Command Default 15 packets

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines A jitter probe, consisting of 2 to 50 packets, details the conditions of the network. More than one packet is used by the probe to calculate an average of delay/loss or Calculated Planning Impairment Factor (ICPIF). After the packets return to the probe, the probe delivers the traffic information to the cache where it is logged for call acceptance/denial. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters. The newly specified number of packets take effect only for new probes.

To get a more realistic estimate on the network congestion, increase the number of packets. If more probing packets are sent, better estimates of network conditions are obtained, but the bandwidth for other network operations is negatively affected. Use fewer packets when you need to maximize bandwidth.

Examples The following example specifies 20 packets in a jitter probe:

```
Router(config)# call fallback jitter-probe num-packets 20
```

Related Commands

Command	Description
call fallback threshold icpif	Specifies the ICPIF threshold.
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.

call fallback jitter-probe precedence

To specify the priority of the jitter-probe transmission, use the **call fallback jitter-probe precedence** command in global configuration mode. To restore the default priority, use the **no** form of this command.

call fallback jitter-probe precedence *precedence-value*

no call fallback jitter-probe precedence

Syntax Description

precedence-value	Jitter-probe precedence. Range is from 0 to 6. The default is 2.

Defaults

Enabled
Value set to 2

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

Every IP packet has a precedence header. Precedence is used by various queueing mechanisms in routers to determine the priority of traffic passing through the system.

Use the **call fallback jitter-probe precedence** command if there are different queueing mechanisms in your network. Enabling the **call fallback jitter-probe precedence** command sets the precedence for jitter probes to pass through your network.

If you require your probes to be sent and returned quickly, set the *precedence* to a low number (0 or 1): the lower the precedence, the higher the priority given.

The **call fallback jitter-probe precedence** command is mutually exclusive with the **call fallback jitter-probe dscp** command. Only one of these commands can be enabled on the router. Usually the **call fallback jitter-probe precedence** command is enabled. When the **call fallback jitter-probe dscp** command is configured, the precedence value is replaced by the DSCP value. To disable DSCP and restore the default jitter probe precedence value, use the **no call fallback jitter-probe dscp** command.

Examples

The following example specifies a jitter-probe precedence of 5, or low priority.

```
call fallback jitter-probe precedence 5
```

The following configuration restores the default value for precedence:

```
no call fallback jitter-probe precedence
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback jitter-probe dscp	Specifies the dscp of the jitter-probe transmission.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
show call fallback config	Displays the call fallback configuration.

call fallback jitter-probe priority-queue

To assign a priority queue for jitter-probe transmissions, use the **call fallback jitter-probe priority-queue** command in global configuration mode. To return to the default state, use the **no** form of this command.

call fallback jitter-probe priority-queue

no call fallback jitter-probe priority-queue

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines This command is applicable only if the queueing method used is IP Real-Time Transport Protocol (RTP) priority. This command is unnecessary when low latency queueing (LLQ) is used because these packets follow the priority queue path (or not) based on the LLQ classification criteria.

This command works by choosing between sending the probe on an odd or even Service Assurance Agent (SAA) port number. The SAA probe packets go out on randomly selected ports chosen from within the top end of the audio User Datagram Protocol (UDP) defined port range (16384 to 32767). The port pair (RTP Control Protocol [RTCP] port) is selected, and by default, SAA probes for call fallback use the RTCP port (odd) to avoid going into the priority queue, if enabled. If call fallback is configured to use the priority queue, the RTP port (even) is selected.

Examples The following example specifies that a probe be sent to an SAA port:

```
Router(config)# call fallback jitter-probe priority-queue
```

Note In order for this command to have any effect on the probes, the IP priority queueing must be set for UDP voice ports numbered from 16384 to 32767.

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the jitter-probe precedence.
ip rtp priority	Provides a strict priority queueing scheme for delay-sensitive data.
show call fallback config	Displays the call fallback configuration.

call fallback key-chain

To specify the use of message digest algorithm 5 (MD5) authentication for sending and receiving Service Assurance Agents (SAA) probes, use the **call fallback key-chain** command in global configuration mode. To disable MD5, use the **no** form of this command.

call fallback key-chain *name-of-chain*

no call fallback key-chain *name-of-chain*

Syntax Description

name-of-chain	Name of the chain. This name is alphanumeric and case-sensitive text. There is no default value.

Command Default

MD5 authentication is not used.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command is used to enable the SAA probe authentication using MD5. If MD5 authentication is used, the keys on the sender and receiver routers must match.

Examples

The following example specifies “sample” as the fallback key chain:

```
Router(config)# call fallback key-chain sample
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
key chain	Enables authentication for routing protocols by identifying a group of authentication keys.
key-string	Specifies the authentication string for a key.
show call fallback config	Displays the call fallback configuration.

call fallback map address-list

To specify that the call fallback router keep a cache table by IP addresses of distances for several destination peers, use the **call fallback map address-list** command in global configuration mode. To restore the default values, use the **no** form of this command.

call fallback map *map* **target** *ip-address* **address-list** *ip-address1 ... ip-address7*

no call fallback map *map* **target** *ip-address* **address-list** *ip-address1 ... ip-address7*

Syntax Description

map	Fallback map. Range is from 1 to 16. There is no default.
target *ip-address*	Target IP address.
ip-address1 ... ip-address7	Lists the IP addresses that are kept in the cache table. The maximum number of IP addresses is seven.

Command Default

No call fallback maps are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

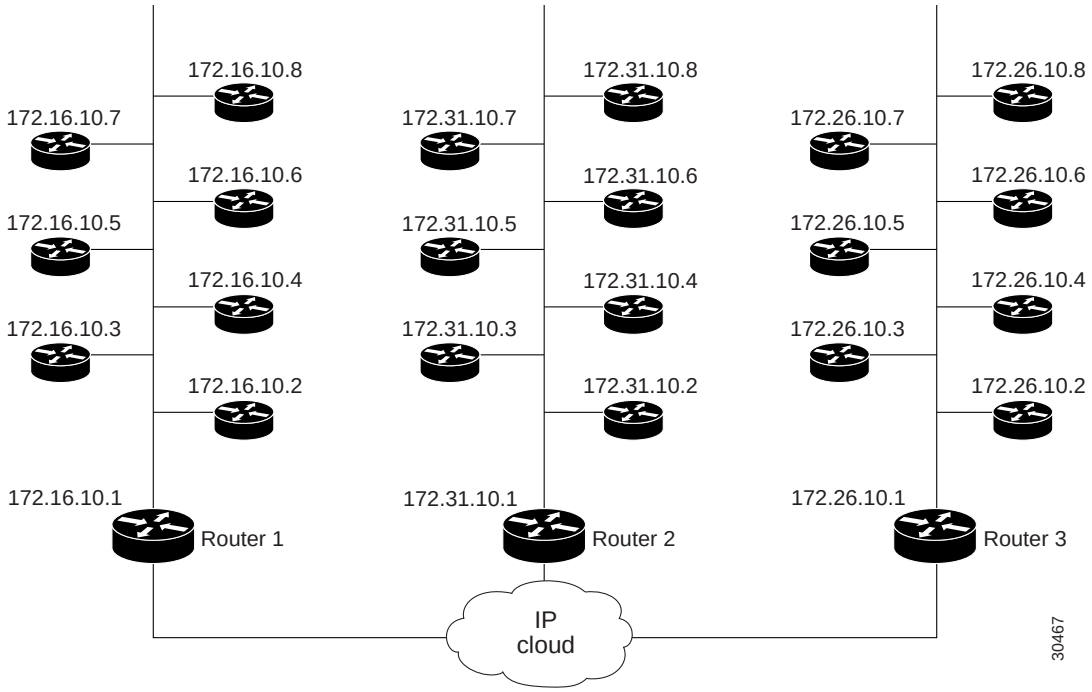
Usage Guidelines

Use this command when several destination peers are in one common node.

Call fallback map setup allows the decongestion of traffic caused by a high volume of call probes sent across a network to query a large number of dial peers. One router/common node can keep the distances in a cache table of the numerous IP addresses/destination peers in a network. When the fallback is queried for network congestion to a particular IP address (that is, the common node), the map addresses are searched to find the target IP address. If a match is determined, the probes are sent to the target address rather than to the particular IP address.

In Figure 1, the three routers (1, 2, and 3) keep the cache tables of distances for the destination peers behind them. When a call probe comes from somewhere in the IP cloud, the cache routers check their distance tables for the IP address/destination peer where the call probe is destined. This distance checking limits congestion on the networks behind these routers by directing the probe to the particular IP address and not to the entire network.

Figure 1 Call Fallback Map with IP Addresses



Examples

The following example specifies call fallback map address-list configurations for 172.32.10.1 and 172.46.10.1:

```
Router(config)# call fallback map 1 target 172.32.10.1 address-list 172.32.10.2
172.32.10.3 172.32.10.4 172.32.10.5 172.32.10.6 172.32.10.7 172.32.10.8

Router(config)# call fallback map 2 target 172.46.10.1 address-list 172.46.10.2
172.46.10.3 172.46.10.4 172.46.10.5 172.46.10.6 172.46.10.7 172.46.10.8
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
show call fallback config	Displays the call fallback configuration.

call fallback map subnet

To specify that the call fallback router keep a cache table by subnet addresses of distances for several destination peers, use the **call fallback map subnet** command in global configuration mode. To restore the default values, use the **no** form of this command.

call fallback map *map* **target** *ip-address* **subnet** *ip-network netmask*

no call fallback map *map* **target** *ip-address* **subnet** *ip-network netmask*

Syntax Description

map	Fallback map. Range is from 1 to 16. There is no default.
target *ip-address*	Target IP address.
subnet *ip-network*	Subnet IP address.
netmask	Network mask number.

Command Default

No call fallback maps are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5850 in this release.

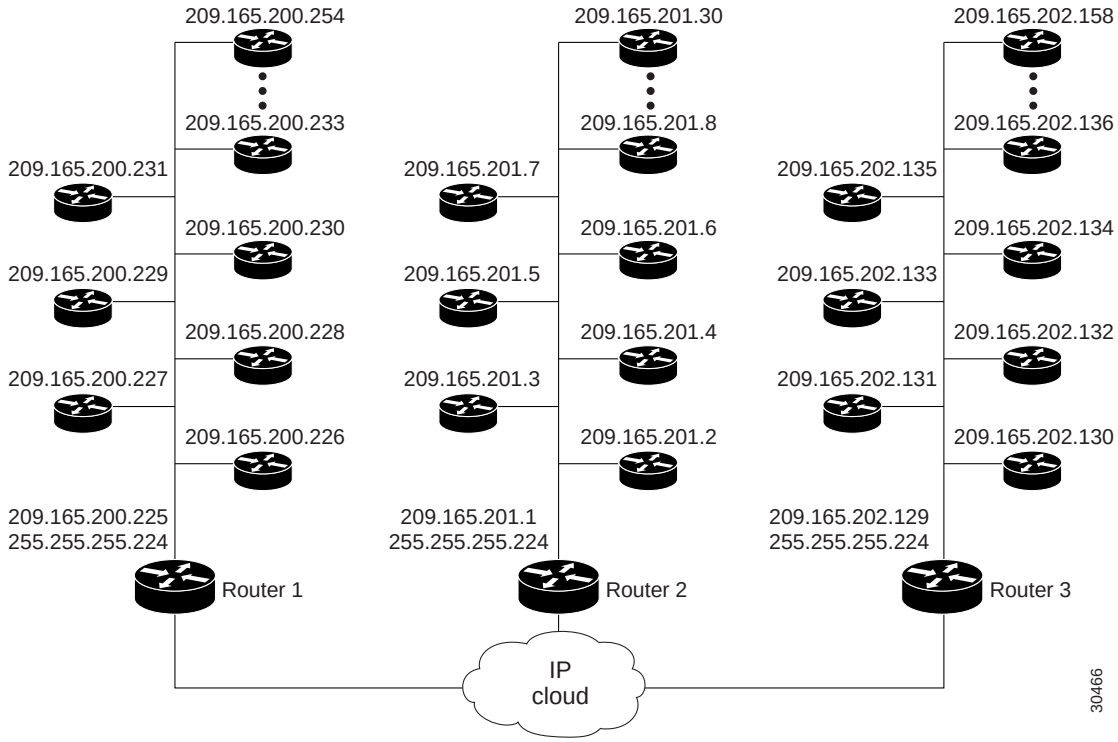
Usage Guidelines

Use this command when several destination peers are in one common node.

Call fallback map setup allows the decongestion of traffic caused by a high volume of call probes sent across a network to query a large number of dial peers. One router/common node can keep the distances in a cache table of the numerous IP addresses within a subnet (destination peers) in a network. When the fallback is queried for network congestion to a particular IP address (that is, the common node), the map addresses are searched to find the target IP address. If a match is determined, the probes are sent to the target address rather than to the particular IP address.

In Figure 2, the three routers (1, 2, and 3) keep the cache tables of distances for the destination peers behind them. When a call probe comes from somewhere in the IP cloud, the cache routers check their distance tables for the subnet address/destination peer where the call probe is destined. This distance checking limits congestion on the networks behind these routers by directing the probe to the particular subnet address and not to the entire network.

Figure 2 Call Fallback Map with Subnet Addresses



Examples

The following examples specify the **call fallback map subnet** configuration for two different IP addresses:

```
Router(config)# call fallback map 1 target 209.165.201.225 subnet
209.165.201.224 255.255.255.224

Router(config)# call fallback map 2 target 209.165.202.225 subnet
209.165.202.224 255.255.255.224
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
show call fallback config	Displays the call fallback configuration.

call fallback monitor

To enable the monitoring of destinations without call fallback to alternate dial peers, use the **call fallback monitor** command in global configuration mode. To disable monitoring without fallback, use the **no** form of this command.

call fallback monitor

no call fallback monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The **call fallback monitor** command is used as a statistics collector of network conditions based upon probes (detailing network traffic) and connected calls. There is no H.323 call checking/rejecting as with the **call fallback active** command. All call requests are granted regardless of network traffic conditions.

Configure the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set threshold parameters. The thresholds are ignored, but for statistics collecting, configuring one of the thresholds allows you to monitor cache entries for either delay/loss or Calculated Planning Impairment Factor (ICPIF) values.

Examples

The following example enables the **call fallback monitor** command:

```
Router(config)# call fallback monitor
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback probe-timeout

To set the timeout for a Service Assurance Agent (SAA) probe for call fallback purposes, use the **call fallback probe-timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback probe-timeout *seconds*

no call fallback probe-timeout

Syntax Description

seconds	Interval, in seconds. Range is from 1 to 2147483. The default is 30.

Command Default

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

SAA probes collect network traffic information based upon configured delay and loss or Calculated Planning Impairment Factor (ICPIF) values and report this information to the cache for call request determination. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.

When the probe timeout expires, a new probe is sent to collect network statistics. To reduce the bandwidth taken up by the probes, increase the probe-timeout interval (*seconds*). Probes do not have a great effect upon bandwidth unless several thousand destinations are involved. If this is the case in your network, use a longer timeout. If you need more network traffic information, and bandwidth is not an issue, use a lower timeout. The default interval, 30 seconds, is a low timeout.

When the **call fallback cache-timeout** command is configured or expires, new probes are initiated for data collection.

Examples

The following example configures a 120-second interval:

```
Router(config)# call fallback probe-timeout 120
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback reject-cause-code

To enable a specific call fallback reject cause code in case of network congestion, use the **call fallback reject-cause-code** command in global configuration mode. To reset the code to the default of 49, use the **no** form of this command.

call fallback reject-cause-code *number*

no call fallback reject-cause-code

Syntax Description

number	Specifies the cause code as defined in the International Telecommunication Union (ITU) standard Q.850 except the code for normal call clearing, which is code 16. The default is 49. See Table 10 for ITU cause-code numbers.

Command Default

49 (quality of service is unavailable)

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Enabling the **call fallback reject-cause-code** command determines the code to display when calls are rejected because of probing of network conditions.

Note Connected calls are not affected by this command.

Table 10 ITU cause codes and their associated display message and meanings.

Cause Code	Displayed Message	Meaning
1	Unallocated (unassigned) number	Indicates that the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates that the equipment that is sending this code has received a request to route the call through a particular transit network that it does not recognize. The equipment that is sending this code does not recognize the transit network either because the transit network does not exist or because that particular transit network, although it does exist, does not serve the equipment that is sending this cause. This code is supported on a network-dependent basis.

Table 10 ITU cause codes and their associated display message and meanings. (continued)

Cause Code	Displayed Message	Meaning
3	No route to destination	Indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This code is supported on a network-dependent basis.
4	Send special information tone	Indicates that the called party cannot be reached for reasons that are of a long-term nature and that the special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.
7	Call awarded and being delivered in an established channel	Indicates that the user has been awarded the incoming call and that the incoming call is being connected to a channel that is already established to that user for similar calls (for example, packet-mode X.25 virtual calls).
8	Preemption	Indicates that the call is being preempted.
9	Preemption - circuit reserved for reuse	Indicates that the call is being preempted and that the circuit is reserved for reuse by the preempting exchange.
16	Normal call clearing	Indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this code is not the network.
17	User busy	Indicates that the called party is unable to accept another call. The user busy code may be generated by the called user or by the network. If the called user generates the user busy code, it is noted that the user equipment is compatible with the call.
18	No user responding	Indicates when a called party does not respond to a call establishment message with either an alerting or a connect indication within the prescribed period of time allocated.
19	No answer from user (user alerted)	Indicates when the called party has been alerted but does not respond with a connect indication within a prescribed period of time. **Note** This code is not necessarily generated by ITU standard Q.931 procedures but may be generated by internal network timers.
20	Subscriber absent	Indicates when a mobile station has logged off, when radio contact is not obtained with a mobile station, or when a personal telecommunication user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates that the equipment that is sending this code does not want to accept this call although it could have accepted the call because the equipment that is sending this code is neither busy nor incompatible. The network may also generate this code, indicating that the call was cleared because of a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.
22	Number changed	Indicates when the called-party number indicated by the calling party is no longer assigned. The new called-party number may be included in the diagnostic field. If a network does not support this code, codeNo. 1, an unallocated (unassigned) number, shall be used.
26	Non-selected user clearing	Indicates that the user has not been sent the incoming call.

Table 10 ITU cause codes and their associated display message and meanings. (continued)

Cause Code	Displayed Message	Meaning
27	Destination out of order	Indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote party; for example, a physical layer or data link layer failure at the remote party, or the equipment of the user is offline.
28	Invalid number format (address incomplete)	Indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.
29	Facility rejected	Indicates when a supplementary service requested by the user cannot be provided by the network.
30	Response to STATUS ENQUIRY	Indicates when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.
31	Normal, unspecified	Reports a normal event only when no other code in the normal class applies.
34	No circuit/channel available	Indicates that no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; for example, immediately reattempting the call is not likely to be successful.
39	Permanent frame mode connection out-of-service	Indicates in a STATUS message that a permanently established frame mode connection is out-of-service (for example, due to equipment or section failure) (see the ITU standard, Annex A/Q.933).
40	Permanent frame mode connection operational	Indicates in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information (see the ITU standard, Annex A/Q.933).
41	Temporary failure	Indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; for example, the user may want to try another call attempt almost immediately.
42	Switching equipment congestion	Indicates that the switching equipment that is generating this code is experiencing a period of high traffic.
43	Access information discarded	Indicates that the network could not deliver access information to the remote user as requested, that is, user-to-user information, low layer compatibility, high layer compatibility, or subaddress, as indicated in the diagnostic. It is noted that the particular type of access information discarded is optionally included in the diagnostic.
44	Requested circuit/channel not available	Indicates when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
46	Precedence call blocked	Indicates that there are no preemptable circuits or that the called user is busy with a call of an equal or higher preemptable level.
47	Resource unavailable, unspecified	Reports a resource-unavailable event only when no other cause in the resource-unavailable class applies.
49	Quality of service not available	Reports that the requested quality of service, as defined in ITU recommendation X.213, cannot be provided (for example, throughput or transit delay cannot be supported).

Table 10 ITU cause codes and their associated display message and meanings. (continued)

Cause Code	Displayed Message	Meaning
50	Requested facility not subscribed	Indicates that the user has requested a supplementary service that is implemented by the equipment that generated this cause but that the user is not authorized to use this service.
53	Outgoing calls barred within CUG	Indicates that, although the calling party is a member of the closed user group (CUG) for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.
55	Incoming calls barred within CUG	Indicates that, although the called party is a member of the CUG for the incoming CUG call, incoming calls are not allowed for this member of the CUG.
57	Bearer capability not authorized	Indicates that the user has requested a bearer capability that is implemented by the equipment that generated this cause but that the user is not authorized to use this capability.
58	Bearer capability not presently available	Indicates that the user has requested a bearer capability that is implemented by the equipment that generated this cause but that is not available at this time.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates that there is an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Reports a service or option not available event only when no other cause in the service or option not available class applies.
65	Bearer capability not implemented	Indicates that the equipment that is sending this code does not support the bearer capability requested.
66	Channel type not implemented	Indicates that the equipment that is sending this code does not support the channel type requested.
69	Requested facility not implemented	Indicates that the equipment that is sending this code does not support the requested supplementary service.
70	Only restricted digital information bearer capability is available (national use)	Indicates that the calling party has requested an unrestricted bearer service but that the equipment that is sending this cause supports only the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Reports a service or option not implemented event only when no other code in the service or option not implemented class applies.
81	Invalid call reference value	Indicates that the equipment that is sending this code has received a message with a call reference that is not currently in use on the user-network interface.
82	Identified channel does not exist	Indicates that the equipment that is sending this code has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a PRI numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.
83	A suspended call exists, but this call identity does not	Indicates that a call resume has been attempted with a call identity that differs from that in use for any suspended calls.
84	Call identity in use	Indicates that the network has received a call suspended request that contains a call identity (including the null call identity) that is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

Table 10 ITU cause codes and their associated display message and meanings. (continued)

Cause Code	Displayed Message	Meaning
85	No call suspended	Indicates that the network has received a call resume request that contains a call identity information element that does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
86	Call having the requested call identity has been cleared	Indicates that the network has received a call resume request that contains a call identity information element that indicates a suspended call that has in the meantime been cleared while suspended (either by network timeout or by the remote user).
87	User not member of CUG	Indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber that is calling a CUG subscriber.
88	Incompatible destination	Indicates that the equipment that is sending this code has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (for example, data rate) that cannot be accommodated.
90	Non-existent CUG	Indicates that the specified CUG does not exist.
91	Invalid transit network selection (national use)	Indicates that a transit network identification was received that is of an incorrect format as defined in ITU standard Annex C/Q.931.
95	Invalid message, unspecified	Reports an invalid message event only when no other code in the invalid message class applies.
96	Mandatory information element is missing	Indicates that the equipment that is sending this code has received a message that is missing an information element that must be present in the message before that message can be processed.
97	Message type non-existent or not implemented	Indicates that the equipment that is sending this code has received a message with a message type that it does not recognize because this is a message not defined or defined but not implemented by the equipment that is sending this cause.
98	Message not compatible with call state or message type non-existent or not implemented	Indicates that the equipment that is sending this code has received a message that the procedures do not indicate as a permissible message to receive while in the call state, or that a STATUS message that indicates an incompatible call state was received.
99	Information element/parameter non-existent or not implemented	Indicates that the equipment that is sending this code has received a message that includes information elements or parameters not recognized because the information element identifiers or parameter names are not defined or are defined but not implemented by the equipment sending the code. This code indicates that the information elements or parameters were discarded. However, the information element is not required to be present in the message for the equipment that is sending the code to process the message.
100	Invalid information element contents	Indicates that the equipment that is sending this code has received an information element that it has implemented; however, one or more fields in the information element are coded in a way that has not been implemented by the equipment that is sending this code.
101	Message not compatible with call state	Indicates that a message has been received that is incompatible with the call state.
102	Recovery on timer expired	Indicates that a procedure has been initiated by the expiration of a timer in association with error-handling procedures.

Table 10 ITU cause codes and their associated display message and meanings. (continued)

Cause Code	Displayed Message	Meaning
103	Parameter non-existent or not implemented - passed on	Indicates that the equipment that is sending this code has received a message that includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment that is sending the code. The code indicates that the parameters were ignored. In addition, if the equipment that is sending this code is an intermediate point, this code indicates that the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates that the equipment that is sending this code has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other code in the protocol error class applies.
127	Interworking, unspecified	Indicates that there has been interworking with a network that does not provide codes for actions it takes. Thus, the precise code for a message that is being sent cannot be ascertained.

Examples

The following example enables the **call fallback reject-cause-code** command and specifies cause code 34:

```
call fallback reject-cause-code 34
```

Related Commands

Command	Description
call fallback cache-size	Specifies the call fallback cache size for network traffic probe entries.
call fallback cache-timeout	Specifies the time after which the cache entries of network conditions are purged.
call fallback instantaneous-value-weight	Specifies that the call fallback subsystem take an average from the last two cache entries for call requests.
call fallback jitter-probe num-packets	Specifies the number of packets in a jitter probe that are used to determine network conditions.
call fallback jitter-probe precedence	Specifies the priority of the jitter-probe transmission.
call fallback jitter-probe priority-queue	Assigns a priority queue for jitter-probe transmissions.
call fallback key-chain	Specifies MD5 authentication for sending and receiving SAA probes.
call fallback map address-list	Specifies that the call fallback router keep a cache table by IP addresses of distances for several destination peers that are sitting behind the router.
call fallback map subnet	Specifies that the call fallback router keep a cache table by subnet addresses of distances for several destination peers that are sitting behind the router.
call fallback probe-timeout	Sets the timeout for an SAA probe for call fallback purposes.

Command	Description
call fallback threshold delay loss	Specifies that the call fallback threshold use only packet delay and loss values.
call fallback threshold icpif	Specifies that call fallback use the ICPIF threshold.
show call fallback config	Displays the call fallback configuration.

call fallback threshold delay loss

To specify that the call fallback threshold use only packet delay and loss values, use the **call fallback threshold delay loss command in** global configuration mode. To restore the default value, use the **no** form of this command.

call fallback threshold delay *milliseconds* **loss** *percent*

no call fallback threshold delay *milliseconds* **loss** *percent*

Syntax Description

milliseconds	The delay value, in milliseconds (ms). Range is from 1 to 2147483647. There is no default value.
percent	The loss value, expressed as a percentage. The valid range is from 0 to 100. There is no default value.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines During times of heavy voice traffic, two parties in a conversation may notice a significant delay in transmission or hear only part of a conversation because of voice-packet loss.

Use the **call fallback threshold delay loss** command to configure parameters for voice quality. Lower values of delay and loss allow higher quality of voice. Call requests match the network information in the cache with the configured thresholds of delay and loss.

The amount of delay set by the **call fallback threshold delay loss** command should not be more than half the amount of the time-to-wait value set by the **call fallback wait-timeout** command; otherwise the threshold delay will not work correctly. Because the default value of the **call fallback wait-timeout** command is set to 300 ms, the user can configure a delay of up to 150 ms for the **call fallback threshold delay loss** command. If the user wants to configure a higher threshold, the time-to-wait delay has to be increased from its default (300 ms) using the **call fallback wait-timeout** command.

Note The delay configured by the **call fallback threshold delay loss** command corresponds to a one-way delay, whereas the time-to-wait period configured by the **call fallback wait-timeout** command corresponds to a round-trip delay.

If you enable the **call fallback active** command, the call fallback subsystem uses the last cache entry compared with the configured delay/loss threshold to determine whether the call is connected or denied. If you enable the **call fallback monitor** command, all calls are connected, regardless of the configured threshold or voice quality. In this case, configuring the **call fallback threshold delay loss** command allows you to collect network statistics for further tracking.

Note The **call fallback threshold delay loss** command differs from the **call fallback threshold icpif** command because the **call fallback threshold delay loss** command uses only packet delay and loss parameters, and the **call fallback threshold icpif** command uses packet delay and loss parameters plus other International Telecommunication Union (ITU) G.113 factors to gather impairment information.

Setting this command does not affect bandwidth. Available bandwidth for call requests is determined by the call fallback subsystem using probes. The number of probes on the network affects bandwidth.

Examples

The following example configures a threshold delay of 20 ms and a threshold loss of 50 percent:

```
Router(config)# call fallback threshold delay 20 loss 50
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback monitor	Enable the monitoring of destinations without call fallback to alternate dial peers.
call fallback threshold icpif	Specifies the ICPIF threshold.
call fallback wait-timeout	Specifies the time to wait for a response to a probe.
show call fallback config	Displays the call fallback configuration.

call fallback threshold icpif

To specify that call fallback use the Calculated Planning Impairment Factor (ICPIF) threshold, use the **call fallback threshold icpif** command in global configuration mode. To restore the default value, use the **no** form of this command.

call fallback threshold icpif *threshold-value*

no **call fallback threshold icpif**

Syntax Description

threshold-value	Threshold value. Range is from 0 to 34. The default is 5.

Command Default 5

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were introduced on the Cisco 7200 series routers and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(8)T	Support for the Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines During times of heavy voice traffic, the parties in a conversation may notice a significant delay in transmission or hear only part of a conversation because of voice-packet loss.

Use the **call fallback threshold icpif** command to configure parameters for voice quality. A low ICPIF value allows for higher quality of voice. Call requests match the network information in the cache with the configured ICPIF threshold. If you enable the **call fallback active** command, the call fallback subsystem uses the last cache entry compared with the configured ICPIF threshold to determine whether the call is connected or denied. If you enable **the call fallback monitor** command, all calls are connected regardless of the configured threshold or voice quality. In this case, configuring the **call fallback threshold icpif** command allows you to collect network statistics for further tracking.

A lower ICPIF value tolerates less delay and loss of voice packets (according to ICPIF calculations). Use lower values for higher quality of voice. Configuring a value of 34 equates to 100 percent packet loss.

The ICPIF is calculated and used according to the International Telecommunication Union (ITU) G.113 specification.

Note The **call fallback threshold delay loss** command differs from the **call fallback threshold icpif** command because the **call fallback threshold delay loss** command uses only packet delay and loss parameters, while the **call fallback threshold icpif** command uses packet delay and loss parameters plus other ITU G.113 factors to gather impairment information.

Setting this command does not affect bandwidth. Available bandwidth for call requests is determined by the call fallback subsystem using probes. The number of probes on the network affects bandwidth.

Examples

The following example sets the **ICPIF threshold** to 20:

```
Router(config)# call fallback threshold icpif 20
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
call fallback monitor	Enables the monitoring of destinations without call fallback to alternate dial peers.
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.
show call fallback config	Displays the call fallback configuration.

call fallback wait-timeout

To modify the time to wait for a response to a probe, use the **call fallback wait-timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

call fallback wait-timeout *milliseconds*

no call fallback wait-timeout *milliseconds*

Syntax Description

milliseconds	The time-to-wait value in milliseconds (ms). The range is 100 to 3000 milliseconds.

Command Default

300 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T9	This command was introduced.

Usage Guidelines

This command is enabled by default. The time to wait for a response to a probe is set to 300 ms. This command allows the user to modify the amount of time to wait for a response to a probe. The *milliseconds* argument allows the user to configure a time-to-wait value from 100 ms and 3000 ms. A user that has a higher-latency network may want to increase the value of the default timer.

The time-to-wait period set by the **call fallback wait-timeout** command should always be greater than or equal to twice the amount of the threshold delay time set by the **call fallback threshold delay loss** command; otherwise the probe will fail.

Note The delay configured by the **call fallback threshold delay loss** command corresponds to a one-way delay, whereas the time-to-wait period configured by **call fallback wait-timeout** command corresponds to a round-trip delay. The threshold delay time should be set at half the value of the time-to-wait value.

Examples

The following example sets the amount of time to wait for a response to a probe to 200 ms:

```
call fallback wait-timeout 200
```

Related Commands

Command	Description
call fallback threshold delay loss	Specifies the call fallback threshold delay and loss values.

call filter match-list voice

To enter the call filter match list configuration mode and create a call filter match list for debugging voice calls, use the **call filter match-list voice** command in global configuration mode. To remove the filter, use the **no** form of this command.

call filter match-list *number* **voice**

no call filter match-list *number* **voice**

Syntax Description

number	Numeric label that uniquely identifies the match list. Range is 1 to 16.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Configure the **call filter match-list voice** command to set the conditions for filtering voice call debugging. After the conditions are set with this command, use the **debug condition match-list** command in privileged EXEC mode to get the filtered debug output.

Examples The following example shows that the call filter match list designated as list 1 filters the debug output for an incoming calling number matching 8288807, an incoming called number matching 6560729, and on incoming port 7/0:D:

```
call filter match-list 1 voice
 incoming calling-number 8288807
 incoming called-number 6560729
 incoming port 7/0:D
```

Related Commands

Command	Description
debug condition match-list	Runs a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.

call forward all

To define a a feature code for a Feature Access Code (FAC) to access Call Forward All (CFA) on an analog phone, use the **call forward all** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

call forward all *keypad-character*

no call forward all

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 1. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.5(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

The default value of the feature code for CFA is 1.

Command Modes

STC application feature access-code configuration (config-stcapp-fac).

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	This command was modified. The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Call Forward All from the default (1) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another FAC, for a speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, by a speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for Call Forward All from the default (1). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the keypad and then dial a target number, to forward all incoming calls to the target number.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# call forward all 3
Router(config-stcapp-fac)# exit
```

The following example shows how to configure all-numeric three or four digit flexible feature access codes so that users are not required to dial a prefix or special characters:

```
VG224(config-stcapp-fac)# call forward all 111
do not use prefix. call forward all is 111
```

Related Commands

Command	Description
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.
call forward cancel	Defines a feature code for a feature access code (FAC) to cancel the call-forward-all condition.
call forward to voicemail	Configures call forwarding to voicemail so that all incoming calls are forwarded to voicemail.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).

Command	Description
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

call forward cancel

To define a a feature code for a Feature Access Code (FAC) to access Call Forward All Cancel, use the **call forward cancel** command in STC application feature access-code configuration mode. To return the feature code to its default, use the **no** form of this command.

call forward cancel *keypad-character*

no call forward cancel

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 2. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default The default value of the feature code is 2.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Call Forward All Cancel from the default (2) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another FAC, for a speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, by a speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Note To disable call-forward-all on a particular directory number associated with SCCP endpoints connected to Cisco Unified CME through an analog voice gateway, use the **no call-forward all** command in ephone-dn or ephone-dn-template configuration mode.

Examples

The following example shows how to change the value of the feature code for Call Forward Cancel from the default (2). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the phone keypad to cancel all-call forwarding.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# call forward cancel 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
call forward all	Defines the feature code in the feature access code (FAC) for forwarding all calls.
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).

Command	Description
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

call-forward-to-voicemail

To configure forwarding of calls to voicemail so that all incoming calls to a directory number are forwarded to voicemail, use the **forward-to-voicemail** command. The **stcapp feature access-code** command must be enabled on the Cisco voice gateway. To disable call forwarding, use the **no** form of this command.

forward-to-voicemail *forward-to-voicemail-code*

no forward-to-voicemail

Syntax Description

forward-to-voicemail-code	Default prefix and code is **7.
keypad-character	In Cisco IOS Release 15.0(1)M and later releases, the string can be either of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

Call forwarding to voicemail is not set.

Command Modes

STC application feature access-code configuration (config-stcapp-fac).

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(11)T	Cisco Unified CME 4.0(3)	This command was introduced.
15.0(1)M	—	This command was modified. The default user behavior of the feature access code was modified.

Usage Guidelines

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

The FAC for forward-to-voicemail follows the same rules as for other FAC, such as **call forward all,** in terms of allowable string as its FAC code.

Examples

The following example show how to configure forward-to-voicemail using a four digit code:

```
VG224(config-stcapp-fac)# forward-to-voicemail 1234
do not use prefix. forward-to-voicemail is 1234
```

Related Commands

Command	Description
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.
call forward cancel	Defines a feature code for a FAC to cancel the call-forward-all condition.
show stcapp feature codes	Displays all FACs.
stcapp feature access-code	Enables FACs and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

call history max

To retain call history information and to specify the number of call records to be retained, use the **call history max** command in global configuration mode.

call history max *number*

Syntax Description

number	The maximum number of call history records to be retained in the history table. Values are from 0 to 1200. The default is 15.

Command Default

If this command is not configured, no call history is maintained for disconnected calls. If the command is configured, the default value for number of records is 15.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The number of disconnected calls displayed is the number specified in the number argument. This maximum number helps to reduce CPU usage in the storage and reporting of this information.

Examples

The following example configures the history table on the gatekeeper to retain 25 records:

```
Router# call history max 25
```

Related Commands

Command	Description
show call history voice	Displays historical information on disconnected calls.

call-history-mib

To define the history MIB parameters, use the **call-history-mib** command in global configuration mode. To disable the configured parameters, use the **no** form of this command.

call-history-mib {**max-size** *num-of-entries* | **retain-timer** *seconds*}

no call-history-mib {**max-size** *num-of-entries* | **retain-timer** *seconds*}

Syntax Description

max-size	Specifies the maximum size of the call history MIB table.
number-of-entries	Number of entries in the call history MIB table. The valid range is from 0 to 500. The default value is 100.
retain-timer	Specifies the timer for entries in the call history MIB table.
seconds	Time in minutes, for removing an entry. The valid range is from 0 to 500. The default time is 15 minutes.

Command Default

The default values are set if the command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

CISCO-CALL-HISTORY-MIB describes the objects defined and used for storing the call information for all calls. The MIB contains a table that stores the past call information. The call information will include the destination number, the call connect time, the call disconnect time and the disconnection cause. These calls could be circuit switched or they could be virtual circuits. The history of each call will be stored. An entry will be created when a call gets disconnected. At the time of creation, the entry will contain the connect time and the disconnect time and other call information.

The history table is characterized by two values, the maximum number (*number-of-entries*) of entries that could be stored in a period of time (*seconds*).

The **max-size** value specifies the maximum size of the call history MIB table.

The **retain-timer** value specifies the length of time, in minutes, that entries will remain in the call history MIB table. Setting the value to 0 prevents any call history from being retained.

Examples

The following examples shows how to set call history MIB parameters:

```
Router# configure terminal
Router(config)# call-history-mib max-size 250
Router# configure terminal
Router(config)# call-history-mib retain-timer 250
```

Related Commands

Command	Description
show startup-config	Displays the contents of the startup configuration file.

call language voice

To configure an external Tool Command Language (Tcl) module for use with an interactive voice response (IVR) application, use the **call language voice command in** global configuration mode.

call language voice *language url*

Syntax Description

language	Two-character abbreviation for the language; for example, "**en**" for English or "**ru**" for Russian.
url	URL that points to the Tcl module.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This is obsolete in Cisco IOS Release 12.3(14)T. Use the **param language** command in application parameter configuration mode.

Usage Guidelines The built-in languages are English (*en)*, Chinese (*ch)*, and Spanish (*sp)*. If you specify "**en**", "**ch**", or **sp**", the new Tcl module replaces the built-in language functionality. When you add a new Tcl module, you create your own prefix to identify the language. When you configure and load the new languages, any upper-layer application (Tcl IVR) can use the language.

You can use the language abbreviation in the *language* argument of any **call application voice** command. The language and the text-to-speech (TTS) notations are available for the IVR application to use after they are defined by the Tcl module.

Examples The following example adds Russian (**ru**) as a Tcl module:

```
call language voice ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
```

Related Commands

Command	Description
call application voice	Configures an application.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
param language	Configures the language parameter in a service or package on the gateway.
show language voice	Displays information about configured languages and applications.

call language voice load

To load or reload a Tool Command Language (Tcl) module from the configured URL location, use the **call language voice load** command in EXEC mode.

call language voice load *language*

Syntax Description

language	The two-character prefix configured with the **call language voice** command in global configuration mode; for example, "en" for English or "ru" for Russian.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines You cannot use this command if the interactive voice response (IVR) application using the language that you want to configure has an active call. A language that is configured under an IVR application is not necessarily in use. To determine if a call is active, use the **show call application voice** command.

Examples The following example loads French (fr) into memory:

```
call language voice load fr
```

Related Commands

Command	Description
call application voice load	Loads an application.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
show language voice	Displays information about configured languages and applications.

call leg dump event-log

To flush the event log buffer for call legs to an external file, use the **call leg dump event-log** command in privileged EXEC mode.

call leg dump event-log

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command immediately writes the event log buffer to the external file whose location is defined with the **call leg event-log dump ftp** command in global configuration mode.

Note The **call leg dump event-log** command and the **call leg event-log dump ftp** command are two different commands.

Examples

The following example writes the event log buffer to an external file named leg_elogs:

```
Router(config)# call leg event-log dump ftp ftp-server/elogs/leg_elogs.log username myname
password 0 mypass
Router(config)# exit
Router# call leg dump event-log
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log

To enable event logging for voice, fax, and modem call legs, use the **call leg event-log** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log

no call leg event-log

Syntax Description This command has no arguments or keywords.

Command Default Event logging for call legs is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines This command enables event logging for telephony call legs. IP call legs are not supported.

Note To prevent event logging from adversely impacting system performance for production traffic, the system includes a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory on the gateway and enable event logging only when necessary to isolate faults.

Examples The following example enables event logging for all telephony call legs:

```
call leg event-log
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.

Command	Description
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log dump ftp

To enable the gateway to write the contents of the call-leg event log buffer to an external file, use the **call leg event-log dump ftp** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log dump ftp *server*[**:***port*]**/***file* **username** *username* **password** [*encryption-type*] *password*

no call leg event-log dump ftp

Syntax Description

server	Name or IP address of FTP server where the file is located.
port	(Optional) Specific port number on server.
file	Name and path of file.
username	Username required for accessing file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. 0 disables encryption; 7 enables encryption. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password	Password required for accessing the file.

Command Default Event logs are not written to an external file.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines This command enables the gateway to automatically write the event log buffer to the named file either after an active call leg terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **call leg event-log max-buffer-size** command. To manually flush the event log buffer, use the **call leg dump event-log** command in privileged EXEC mode.

Note The **call leg dump event-log** command and the **call leg event-log dump ftp** command are two different commands.

Note Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Examples

The following example enables the gateway to write call leg event logs to an external file named leg_elogs.log on a server named ftp-server:

```
call leg event-log dump ftp ftp-server/elogs/leg_elogs.log username myname password 0
mypass
```

The following example specifies that call leg event logs are written to an external file named leg_elogs.log on a server with the IP address 10.10.10.101:

```
call leg event-log dump ftp 10.10.10.101/elogs/leg_elogs.log username myname password 0
mypass
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log errors-only

To restrict event logging to error events only for voice call legs, use the **call leg event-log errors-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log errors-only

no call leg event-log errors-only

Syntax Description This command has no arguments or keywords.

Command Default All call leg events are logged.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines This command limits the severity level of the events that are logged; it does not enable logging. You must use this command with the **call leg event-log** command, which enables event logging for call legs.

Examples The following example shows how to capture event logs only for call legs with errors:

```
Router(config)# call leg event-log
Router(config)# call leg event-log errors-only
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg event-log max-buffer-size

To set the maximum size of the event log buffer for each call leg, use the **call leg event-log max-buffer-size** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg event-log max-buffer-size *kbytes*

no call leg event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes (KB). Range is 1 to 20. Default is 4.

Command Default

4 KB

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call leg** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **call leg event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **call leg event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Examples

The following example sets the maximum buffer size to 8 KB:

```
call leg event-log max-buffer-size 8
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
monitor call leg event-log	Displays the event log for an active call leg in real-time.
show call leg	Displays event logs and statistics for voice call legs.

call leg history event-log save-exception-only

To save to history only event logs for call legs that had at least one error, use the **call leg history event-log save-exception-only** command in global configuration mode. To reset to the default, use the **no** form of this command.

call leg history event-log save-exception-only

no call leg history event-log save-exception-only

Syntax Description

This command has no arguments or keywords.

Command Default

By default all the events will be logged.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Call leg event logs move from the active to the history table after the call leg terminates. If you use this command, event logs are saved only for those legs that had errors. Event logs for normal legs that do not contain any errors are not saved.

Note This command does not affect records saved to an FTP server by using the **call leg dump event-log** command.

Examples

The following example saves to history only call leg records that have errors:

```
call leg history event-log save-exception-only
```

Related Commands

Command	Description
call leg dump event-log	Flushes the event log buffer for call legs to an external file.
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
show call leg	Displays event logs and statistics for voice call legs.

callmonitor

To enable call monitoring messaging functionality on a SIP endpoint in a VoIP network, use the **callmonitor** command in voice-service configuration mode. To return to the default, use the **no** form of this command.

callmonitor

no callmonitor

Syntax Description

This command has no arguments or keywords.

Command Default

Monitoring service is disabled.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Cisco IOS Release	Modification
12.4(11)XW2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command in voice service configuration mode to allow a SIP endpoint, such as an external feature server, to watch call activity on a VoIP network.

To view call activity, use the **show callmon** command.

Examples

The following example enables call monitoring messaging functionality on a SIP endpoint:

```
Router(config-voi-serv)# callmonitor
```

Related Commands

Command	Description
show callmon	Displays call-monitor information.

call preserve

To enable the preservation of H.323 VoIP calls, use the **call preserve** command in h323, voice-class h323, and voice service voip configuration modes. To reset to the default, use the **no** form of this command.

call preserve [**limit-media-detection**]

no call preserve [**limit-media-detection**]

Syntax Description

limit-media-detection	Limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to H.323 VoIP preserved calls only.

Command Default

H.323 VoIP call preservation is disabled.

Command Modes

h323, voice-class h323, or voice service voip

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **call preserve** command activates H.323 VoIP call preservation for following types of failures and connections:

Failure Types

- WAN failures that include WAN links flapping or degraded WAN links
- Cisco Unified CallManager software failure, such as when the ccm.exe service crashes on a Cisco Unified CallManager server.
- LAN connectivity failure, except when a failure occurs at the local branch

Connection Types

- Calls between two Cisco Unified CallManager controlled endpoints
  - During Cisco Unified CallManager reloads
  - When a Transmission Control Protocol (TCP) connection between one or both endpoints and Cisco Unified CallManager used for signaling H.225.0 or H.245 messages is lost or flapping
  - Between endpoints that are registered to different Cisco Unified CallManagers in a cluster and the TCP connection between the two Cisco Unified CallManagers is lost
  - Between IP phones and the PSTN at the same site
- Calls between Cisco IOS gateway and an endpoint controlled by a softswitch where the signaling (H.225.0, H.245 or both) flows between the gateway and the softswitch and media flows between the gateway and the endpoint.

  - When the softswitch reloads.
  - When the H.225.0 or H.245 TCP connection between the gateway and the softswitch is lost, and the softswitch does not clear the call on the endpoint
  - When the H.225.0 or H.245 TCP connection between softswitch and the endpoint is lost, and the soft-switch does not clear the call on the gateway
- Call flows that involve a Cisco IP in IP (IPIP) gateway running in media flow-around mode that reload or lose connection with the rest of the network

When bidirectional silence and RTP and RTCP inactivity detection are configured, they are enabled for all calls by default. To enable them for H.323 VoIP preserved calls only, you must use the **call preserve** command's **limit-media-detection** keyword.

H.323 VoIP call preservation can be applied globally to all calls and to a dial peer.

Examples

The following example enables H.323 VoIP call preservation for all calls.

```
voice service voip
 h323
  call preserve
```

The following configuration example enables H.323 VoIP call preservation for dial peer 1.

```
voice-class h323 4
 call preserve
dial-peer voice 1 voip
 voice-class h323 4
```

The following example enables H.323 VoIP call preservation and enables RTP and RTCP inactivity detection and bidirectional silence detection for preserved calls only:

```
voice service voip
 h323
  call preserve limit-media-detection
```

The following example enables RTP and RTCP inactivity detection. Note that for H.323 VoIP call preservation VAD must be set to off (**no vad** command).

```
dial-peer voice 10 voip
 no vad
gateway
 timer receive-rtcp
ip rtcp report-interval
```

The following configuration example enables bidirectional silence detection:

```
gateway
 timer media-inactive
ip rtcp report interval
```

Related Commands

Command	Description
h323	Enables the H.323 voice service configuration commands.
show h323 calls preserved	Displays data about active H.323 VoIP preserved calls.
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service voip	Enters voice-service configuration mode

call-route

To enable header-based routing, at the global configuration level, use the **call-route** command in voice service VoIP SIP configuration mode. To disable header-based routing, use the **no** form of this command.

call-route {**p-called-party-id** | **history-info**}

no call-route {**p-called-party-id** | **history-info**}

Syntax Description

p-called-party-id	Enables call routing based on the p-called-party-id header.
history-info	Enables call routing based on the history-info header.

Command Default

Support for call routing based on the header in a received INVITE message is disabled.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This keyword was modified. The **history-info** keyword was added.

Usage Guidelines

Use the **call-route** command to enable the Cisco Unified Border Element to route calls based on the P-Called-Party-ID or history-header in a received INVITE message.

Examples

The following example shows how to enable call routing based on the header value:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# call-route p-called-party-id
Router(conf-serv-sip)# call-route history-info
```

Related Commands

Command	Description
voice-class sip call-route	Enables call routing based on the p-called-party-id and history-info header values at the dial-peer configuration level.

call-router h323-annexg

To enable the Annex G border element (BE) configuration commands by invoking H.323 Annex G configuration mode, use the **call-router** command in global configuration mode. To remove the definition of a BE, use the **no** form of this command.

call-router h323-annexg *border-element-id*

no call-router h323-annexg

Syntax Description

border-element-id	Identifier of the BE that you are provisioning. Possible values are any International Alphabet 5 (IA5) string, without spaces and up to 20 characters in length. This value must match the value that you specified for the BE ID in the **border-element** command.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to enter Annex G configuration mode and to identify BEs.

Examples

The following example shows that Annex G configuration mode is being entered for a BE named “be20”:

```
Router(config)# call-router h323-annexg be20
```

Related Commands

Command	Description
show call history	Displays the fax call history table for a fax transmission.
show call-router status	Displays the Annex G BE status.

call-routing hunt-scheme

To enable capacity based load-balancing, use the **call-routing hunt-scheme** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

call-routing hunt-scheme percentage-capacity-util

no call-routing hunt-scheme

Syntax Description

percentage-capacity-util	Selects the one with least percentage capacity utilized among the gateways.

Command Default

This command is disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **call-routing hunt-scheme** command to turn on load balancing based on capacity of gateway and verify that the gateway capacity reporting is enabled.

Examples

The following example shows the gateway with the with least percentage capacity being selected:

```
Router(gk-config)# call-routing hunt-scheme percentage-capacity-util
```

Related Commands

Command	Description
timer cluster-element	Sets the time between resource update messages to gatekeepers in local cluster.

call rscmon update-timer

To change the value of the resource monitor throttle timer, use the **call rscmon update-timer** command in privileged EXEC mode. To revert to the default value, use the **no** form of this command.

call rscmon update-timer *milliseconds*

no call rscmon update-timer

Syntax Description

milliseconds	Duration of the resource monitor throttle timer, in milliseconds (ms). Range is from 20 to 3500. The default is 2000.

Command Default

2000 ms

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command specifies the duration of the resource monitor throttle timer. When events are delivered to the resource monitor process, the throttle timer is started and the event is processed after the timer expires (unless the event is a high-priority event). The timer ultimately affects the time it takes the gateway to send Resource Availability Indicator (RAI) messages to the gatekeeper. This command allows you to vary the timer according to your needs.

Examples

The following example shows how the timer is to be configured:

```
Router(config)# call rscmon update-timer 1000
```

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to its gatekeeper.

call rsvp-sync

To enable synchronization between Resource Reservation Protocol (RSVP) signaling and the voice signaling protocol, use the **call rsvp-sync** command in global configuration mode. To disable synchronization, use the **no** form of this command.

call rsvp-sync

no call rsvp-sync

Syntax Description

This command has no keywords or arguments.

Command Default

Synchronization is enabled between RSVP and the voice signaling protocol (for example, H.323).

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, 3600 series, 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **call rsvp-sync** command is enabled by default.

Examples

The following example enables synchronization between RSVP and the voice signaling protocol:

```
call rsvp-sync
```

Related Commands

Command	Description
call rsvp-sync resv-timer	Sets the timer for reservation requests.
call start	Forces the H.323 Version 2 gateway to use fast connect or slow connect procedures for a dial peer.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
h323 call start	Forces an H.323 Version 2 gateway to use fast connect or slow connect procedures for all VoIP services.
ip rsvp bandwidth	Enables the use of RSVP on an interface.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that have attempted RSVP reservation.

call rsvp-sync resv-timer

To set the timer on the terminating VoIP gateway for completing RSVP reservation setups, use the **call rsvp-sync resv-timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

call rsvp-sync resv-timer *seconds*

no call rsvp-sync resv-timer

Syntax Description

seconds	Number of seconds in which the reservation setup must be completed, in both directions. Range is from 1 to 60. The default is 10.

Command Default 10 seconds

Command Modes Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The reservation timer is started on the terminating gateway when the session protocol receives an indication of the incoming call. This timer is not set on the originating gateway because the resource reservation is confirmed at the terminating gateway. If the reservation timer expires before the RSVP setup is complete, the outcome of the call depends on the acceptable quality of service (QoS) level configured in the dial peer; either the call proceeds without any bandwidth reservation or it is released. The timer must be set long enough to allow calls to complete but short enough to free up resources. The optimum number of seconds depends on the number of hops between the participating gateways and the delay characteristics of the network.

Examples The following example sets the reservation timer to 30 seconds:

```
call rsvp-sync resv-timer 30
```

Related Commands

Command	Description
call rsvp-sync	Enables synchronization of RSVP and the H.323 voice signaling protocol.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that have attempted RSVP reservation.

call service stop

To shut down VoIP call service on a gateway, use the **call service stop** command in voice service SIP or voice service H.323 configuration mode. To enable VoIP call service, use the **no** form of this command. To set the command to its defaults, use the **default call service stop** command

call service stop [**forced**] [**maintain-registration**]

no call service stop

default call service stop

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.
maintain-registration	(Optional) Forces the gateway to remain registered with the gatekeeper.

Command Default

VoIP call service is enabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)
Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(23.08)T01	The default behavior was clarified for SIP and H.323 protocols.

Usage Guidelines

Use the **call service stop** command to shut down the SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **no call service stop** command to enable SIP or H.323 services regardless of whether the **shutdown** or **no shutdown** command was configured in voice service configuration mode.

Use the **default call service stop** command to set the command to its defaults. The defaults are as follows:

- Shut down SIP or H.323 service, if the **shutdown** command was configured in voice service configuration mode.
- Enable SIP or H.323 service, if the **no shutdown** command was configured in voice service configuration mode.

Examples

The following example shows SIP call service being shut down on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# call service stop
```

The following example shows H.323 call service being enabled on a Cisco gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# no call service stop
```

The following example shows SIP call service being enabled on a Cisco gateway because the **no shutdown** command was configured in voice service configuration mode:

```
Router> enable
Router# configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)# no shutdown
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# default call service stop
```

The following example shows H.323 call service being shut down on a Cisco gateway because the **shutdown** command was configured in voice configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# shutdown
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# default call service stop
```

Related Commands

Command	Description
bandwidth audio as-modifier	Allows SIP SDP bandwidth-related options.
billing b-channel	Enables the H.323 gateway to access B-channel information for all H.323 calls.
outbound-proxy	Configures an outbound proxy server.
telephony-service ccm-compatible	Enables the detection of a Cisco CallManager system in the network and allows the exchange of calls.

call spike

To configure the limit on the number of incoming calls received in a short period of time (a call spike), use the **call spike** command in global or dial peer voice configuration mode. To disable this command, use the **no** form of this command.

call spike *call-number* [**steps** *number-of-steps* **size** *milliseconds*]

no call spike

Dial Peer Voice Configuration Mode

call spike *threshold* [**steps** *number-of-steps* **size** *milliseconds*]

Syntax Description

call-number	Incoming call count for the spiking threshold. Range is 1 to 2147483647.
steps *number-of-steps*	(Optional) Specifies the number of steps for the spiking sliding window. Range is from 3 to 10. The default is 5.steps for the spiking sliding window.
size *milliseconds*	(Optional) Specifies step size in milliseconds. Range is from 100 to 250. The default is 200.
threshold	Threshold for the incoming call count for spiking. Range is 1 to 2147483647.

Command Default

The limit on the number of incoming calls received during a specified period is not configured.

Command Modes

Global configuration (config)
Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This release does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms was not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
15.1(3)T	This command was modified. Support for this command was added in the dial peer level.

Usage Guidelines

A call spike occurs when a large number of incoming calls arrive from the Public Switched Telephone Network (PSTN) in a short period of time (for example, 100 incoming calls in 10 milliseconds). Setting this command allows you to control the number of call requests that can be received in a configured time period. The sliding window buffers the number of calls that get through. The counter resets according to the specified step size.

The period of the sliding window is calculated by multiplying the number of steps by the size. If an incoming call exceeds the configured call number during the period of the sliding window the call is rejected.

If the **call spike** is configured at both the global and dial-peer levels, the dial-peer level takes precedence and the call spike is calculated. If the call spike threshold is exceeded the call gets rejected, and the call spike calculation is done at the global level.

Examples

The following example shows how to configure the **call spike** command with a call-number and the of 1, a sliding window of 10 steps, and a step size of 200 milliseconds. The period of the sliding window is 2 seconds. If the gateway receives more than 1 call within 2 seconds the call is rejected.

```
Router(config)# call spike 1 steps 10 size 200
```

The following example shows how to configure the **call spike** command with a call number of 30, a sliding window of 10 steps, and a step size of 2000 milliseconds:

```
Router(config)# call spike 30 steps 10 size 2000
```

The following example shows how to configure the **call spike** command in dial peer voice mode with threshold of 20, a sliding window of 7, and a step size of 2000 milliseconds:

```
Router(config)# dial-peer voice 400 voip
Router(config-dial-peer)# call spike 20 steps 7 size 2000
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
show call spike status	Displays the configuration of the threshold for incoming calls.

call start

To force an H.323 Version 2 gateway to use either fast connect or slow connect procedures for a dial peer, use the **call start** command in H.323 voice-service configuration mode. To restore the default setting, use the **no** form of this command.

call start {**fast** | **slow** | **system** | **interwork**} [**sync-rsvp slow-start**]

no call start

Syntax Description

fast	Gateway uses H.323 Version 2 (fast connect) procedures.
slow	Gateway uses H.323 Version 1 (slow connect) procedures.
system	Gateway defaults to voice-service configuration mode.
interwork	(Optional) Gateway interoperates between fast-connect and slow-connect procedures. **Note** The **interwork** keyword is applicable to IP-to-IP gateways only and supports basic audio calls Dual-tone multi-frequency (DTMF), fax, and audio transcoding calls are not supported).
sync-rsvp slow-start	(Optional) Gateway uses Resource Reservation Protocol (RSVP) synchronization for slow-start calls.

Command Default

system

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was changed to use the H.323 voice-service configuration mode from the voice-class configuration mode.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(4)T	The **synch-rsvp slow-start** keywords were added.
12.3(8)T	The **interwork** keyword was added.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later releases, H.323 VoIP gateways by default use H.323 Version 2 (fast connect) for all calls, including those initiating RSVP. Previously, gateways used only slow-connect procedures for RSVP calls. To enable Cisco IOS Release 12.1(3)XI gateways to be backward-compatible with earlier releases of Cisco IOS Release 12.1T, the **call start** command allows the originating gateway to initiate calls using slow connect.

The **call start** command is configured as part of the voice class assigned to an individual VoIP dial peer. It takes precedence over the **h323 call start** command that is enabled globally to all VoIP calls, unless the **system** keyword is used, in which case the gateway defaults to Version 2.

The **sync-rsvp slow-start keyword**, when used in H.323 voice-class configuration mode, controls RSVP synchronization for all slow-start calls handled by the gateway. When t**he sync-rsvp slow-start keyword is** used in an H.323 voice-class definition, the behavior can be specified for individual dial peers by invoking the voice class in dial-peer voice configuration mode. This command is enabled by default in some Cisco IOS images, and in this situation the **show running-config** command displays this information only when the **no** form of the command is used.

Note The **call start** command supports only H.323 to H.323 calls.

The **interwork** keyword is only used with IP-to-IP gateways connecting fast connect from one side to slow connect on the other for basic audio calls. Configure the **interwork** keyword in voice-class H.323 configuration mode or on both the incoming and outgoing dial peers. Codecs must be specified on both dial peers for interworking to function. When the **interwork** keyword is configured, codecs need to be specified on both dial-peers and the **codec transparent** command should not be configured.

Examples

The following example shows slow connect for the voice class 1000 being selected:

```
voice service class h323 1000
 call start slow
!
dial-peer voice 210 voip
 voice-class h323 1000
```

The following example shows the gateway configured to use the H.323 Version 1 (slow connect) procedures:

```
h323
 call start slow
```

Related Commands

Command	Description
acc-qos	Selects the acceptable quality of service for a dial peer.
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
codec transparent	Enables codec capabilities to be passed transparently between endpoints in a Cisco IPIPGW.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
h323	Enables H.323 voice service configuration commands.
req-qos	Selects the desired quality of service to use in reaching a dial peer.

show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.
show running-config	Displays the contents of the currently running configuration file.
voice class h323	Enters voice-class configuration mode and creates a voice class for H.323 attributes.

call threshold global

To enable the global resources of a gateway, use the **call threshold global** command in global configuration mode. To disable the global resources of the gateway, use the **no** form of this command.

call threshold global *trigger-name* **low** *percent* **high** *percent* [**busyout**] [**treatment**]

no call threshold global *trigger-name*

Syntax Description

trigger-name	Specifies the global resources on the gateway. The *trigger-name* argument can be one of the following: • **cpu-5sec**—CPU utilization in the last 5 seconds. • **cpu-avg**—Average CPU utilization. • **io-mem**—I/O memory utilization. • **proc-mem**—Processor memory utilization. • **total-calls**—Total number of calls. • **total-mem**—Total memory utilization.
low *percent*	Value of low threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for the **total-calls.**
high *percent*	Value of high threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for the **total-calls**.
busyout	(Optional) Busy out the T1/E1 channels if the resource is not available.
treatment	(Optional) Applies call treatment from the session application if the resource is not available.

Command Default

The default is **busyout** and **treatment** for global resource triggers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.

Usage Guidelines

Use this command to enable a trigger and define associated parameters to allow or disallow new calls on the router. Action is enabled when the trigger value goes above the value specified by the **high** keyword and is disabled when the trigger drops below the value specified by the **low** keyword.

You can configure these triggers to calculate Resource Availability Indicator (RAI) information. An RAI is forwarded to a gatekeeper so that it can make call admission decisions. You can configure a trigger that is global to a router or is specific to an interface.

Examples

The following example shows how to busy out the total calls when a low of 5 or a high of 5000 is reached:

```
call threshold global total-calls low 5 high 5000 busyout
```

The following example shows how to busy out the average CPU utilization if a low of 5 percent or a high of 65 percent is reached:

```
call threshold global cpu-avg low 5 high 65 busyout
```

Related Commands

Command	Description
call threshold (interface)	Enables interface resources of a gateway.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.
show call threshold	Displays enabled triggers, current values for configured triggers, and number of API calls that were made to global and interface resources.

call threshold interface

To enable the interface resources of a gateway, use the **call threshold interface** command in global configuration mode. To disable the interface resources of the gateway, use the **no** form of this command.

call threshold interface *name number* **int-calls low** *value* **high** *value*

no call threshold interface *name number* **int-calls**

Syntax Description

name	Specifies the interface name.
number	Number of calls through the interface.
int-calls	Number of calls transmitted through the interface.
low *value*	Low threshold number of calls allowed: Range is 1 to 10000 calls.
high *value*	High threshold numer of calls allowed: Range is 1 to 10000 calls.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to specify thresholds that allow or disallow new calls on the router.

Examples

The following example enables thresholds as low as 5 and as high as 2500 for interface calls on interface Ethernet interface 0/1:

```
call threshold interface Ethernet 0/1 int-calls low 5 high 2500
```

Related Commands

Command	Description
call threshold (global)	Enables global resources of a gateway.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.
show call threshold	Displays enabled triggers, current values for configured triggers, and number of API calls that were made to global and interface resources.

call threshold poll-interval

To enable a polling interval threshold for assessing CPU or memory thresholds, use the **call threshold poll-interval** command in global configuration mode. To disable this command, use the **no** form of this command.

call threshold poll-interval {**cpu-average** | **memory**} *seconds*

no call threshold poll-interval {**cpu-average** | **memory**}

Syntax Description

cpu-average	The CPU average interval, in seconds. The default is 60.
memory	The average polling interval for the memory, in seconds. The default is 5.
seconds	Window of polling interval, in seconds. Range is from 10 to 300 for the CPU average interval, and from 1 to 60 for the memory average polling interval.

Command Default

cpu-average: 60 seconds
memory: 5 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. This release does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This release does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Examples

The following example shows how to specify that memory thresholds be polled every 10 seconds:

```
call threshold poll-interval memory 10
```

Related Commands

Command	Description
call threshold	Enables the global resources of the gateway.
clear call threshold	Clears enabled triggers and their associated parameters.
show call threshold	Displays enabled triggers, current values for configured triggers, and number of API calls that were made to global and interface resources.

call treatment action

To configure the action that the router takes when local resources are unavailable, use the **call treatment action** command in global configuration mode. To disable call treatment action, use the **no** form of this command.

call treatment action{**hairpin** | **playmsg** *url* | **reject**}

no call treatment action

Syntax Description

hairpin	Hairpins the calls through the POTS dial peer. **Note** The **hairpin** keyword is not available on Cisco 1750 and Cisco 1751 routers.
playmsg	Plays a specified message to the caller.
url	Specifies the URL of the audio file to play.
reject	Disconnects the call and pass-down cause code.

Command Default

No treatment is applied.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

Use this command to define parameters to disconnect (with cause code), or hairpin, or whether a message or busy tone is played to the user.

Examples

The following example shows how to enable the call treatment feature with a “hairpin” action:

```
call treatment on
call treatment action hairpin
```

The following example shows how to enable the call treatment feature with a “playmsg” action. The file “congestion.au” plays to the caller when local resources are not available to handle the call.

```
call treatment on
call treatment action playmsg tftp://keyer/prompts/conjestion.au
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment cause-code

To specify the reason for the disconnection to the caller when local resources are unavailable, use the **call treatment cause-code** command in global configuration mode. To disable the call treatment cause-code specification, use the **no** form of this command.

call treatment cause-code {**busy** | **no-QoS** | **no-resource**}

no call treatment cause-code

Syntax Description

busy	Indicates that the gateway is busy.
no-QoS	Indicates that the gateway cannot provide quality of service (QoS).
no-resource	Indicates that the gateway has no resources available.

Command Default Disconnect reason is not specified to the caller.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines Use this command to associate a cause-code with a disconnect event.

Examples The following example shows how to configure a call treatment cause code to reply with “no-Qos” when local resources are unavailable to process a call:

```
call treatment on
call treatment cause-code no-Qos
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment isdn-reject

To specify the rejection cause code for ISDN calls when all ISDN trunks are busied out and the switch ignores the busyout trunks and still sends ISDN calls into the gateway, use the **call treatment isdn-reject** command in global configuration mode. To disable call treatment, use the **no** form of this command.

call treatment isdn-reject *cause-code*

no call treatment isdn-reject

Syntax Description

cause-code	Selects the ISDN reject cause code. Valid entries are as follows:	
	Code	**Description**
	34	No circuit/channel available—The connection cannot be established because no appropriate channel is available to take the call.
	38	Network out of order—The destination cannot be reached because the network is not functioning correctly, and the condition might last for an extended period of time. An immediate reconnect attempt will probably be unsuccessful.
	41	Temporary failure—An error occurred because the network is not functioning correctly. The problem will be resolved shortly.
	42	Switching equipment congestion—The destination cannot be reached because the network switching equipment is temporarily overloaded.
	43	Access information discarded—Discarded information element identifier. The network cannot provide the requested access information.
	44	Requested circuit/channel not available—The remote equipment cannot provide the requested channel for an unknown reason. This might be a temporary problem.
	47	Resources unavailable, unspecified—The requested channel or service is unavailable for an unknown reason. This might be a temporary problem.

Command Default No value is specified.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

Use this command only when all ISDN trunks are busied out and the switch ignores the busyout trunks and still sends ISDN calls into the gateway. The gateway should reject the call in the ISDN stack using the configured cause code.

Under any other conditions, the command has no effect.

Examples

The following example shows how to configure the call treatment to reply to an ISDN call with an ISDN rejection code for “temporary failure” when local resources are unavailable to process a call:

```
call treatment on
call treatment isdn-reject 41
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call treatment on

To enable call treatment to process calls when local resources are unavailable, use the **call treatment on** command in global configuration mode. To disable call treatment, use the **no** form of this command.

call treatment on

no call treatment on

Syntax Description This command has no arguments or keywords.

Command Default Treatment is inactive.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751 routers. This command does not support any other Cisco platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines Use this command to enable a trigger and define associated parameters to disconnect (with cause code), or hairpin, or whether a message or busy tone is played to the user.

Examples The following example shows how to enable the call treatment feature with a “hairpin” action:

```
call treatment on
call treatment action hairpin
```

The following example shows how to enable the call treatment feature with a “playmsg” action. The file “congestion.au” plays to the caller when local resources are not available to handle the call.

```
call treatment on
call treatment action playmsg tftp://keyer/prompts/conjestion.au
```

The following example shows how to configure a call treatment cause code to reply with “no-QoS” when local resources are unavailable to process a call:

```
call treatment on
call treatment cause-code no-QoS
```

Related Commands

Command	Description
call threshold	Clears enabled triggers and their associated parameters.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause-code for ISDN calls when local resources are unavailable.
clear call treatment stats	Clears the call treatment statistics.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

call-waiting

To enable call waiting, use the **call-waiting** command in interface configuration mode. To disable call waiting, use the **no** form of this command.

call-waiting

no call-waiting

Syntax Description This command has no arguments or keywords.

Command Default Call waiting is enabled.

Command Modes Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines This command is applicable to Cisco 800 series routers.

You must specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco 800 Series Routers Software Configuration Guide*.

Examples The following example disables call waiting:

```
no call-waiting
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dial peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show dial peer voice	Displays configuration information and call statistics for dial peers.

called-number (dial peer)

To enable an incoming Voice over Frame Relay (VoFR) call leg to get bridged to the correct plain old telephone service (POTS) call leg when a static FRF.11 trunk connection is used, use the **called-number** command in dial peer configuration mode. To disable a static trunk connection, use the **no** form of this command.

called-number *string*

no called-number

Syntax Description

string	A string of digits, including wildcards, that specifies the telephone number of the voice port dial peer.

Command Default This command is disabled.

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines The **called-number** command is used only when the dial peer type is VoFR and you are using the frf11-trunk (FRF.11) session protocol. It is ignored at all times on all other platforms using the Cisco-switched session protocol.

Because FRF.11 does not provide any end-to-end messaging to manage a trunk, the **called-number** command is necessary to allow the router to establish an incoming trunk connection. The E.164 number is used to find a matching dial peer during call setup.

Examples The following example shows how to configure a static FRF.11 trunk connection to a specific telephone number (555-0150), beginning in global configuration mode:

```
voice-port 1/0/0
 connection trunk 55Router0
 exit

dial-peer voice 100 pots
 destination pattern 5550150
 exit

dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5550150
 destination pattern 55Router0
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
connection	Specifies a connection mode for a voice port.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (VoFR)	Enables the generation of FRF.11 Annex A frames for a dial peer.
fax-rate	Establishes the rate at which a fax is sent to the specified dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
vad (dial peer)	Enables VAD for the calls using a particular dial peer.

caller-id (dial peer)

To enable caller ID, use the **caller-id** command in dial peer configuration mode. To disable caller ID, use the **no** form of the command.

caller-id

no caller-id

Syntax Description This command contains no arguments or keywords.

Command Default Caller ID is disabled

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines This command is available on Cisco 800 series routers that have plain old telephone service (POTS) ports. The command is effective only if you subscribe to caller ID service. If you enable caller ID on a router without subscribing to the caller ID service, caller ID information does not appear on the telephone display.

The configuration of caller ID must match the device connected to the POTS port. That is, if a telephone supports the caller ID feature, use the **caller-id** command to enable the feature. If the telephone does not support the caller ID feature, use the command default or disable the caller ID feature. Odd ringing behavior might occur if the caller ID feature is disabled when it is a supported telephone feature or enabled when it is not a supported telephone feature.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples The following example enables a router to use the caller ID feature:

```
dial-peer voice 1 pots
 caller-id
```

Related Commands

Command	Description
block-caller	Configures call blocking on caller ID.
debug pots csm csm	Activates events from which an application can determine and display the status and progress of calls to and from POTS ports.
isdn i-number	Configures several terminal devices to use one subscriber line.
pots call-waiting	Enables local call waiting on a router.
registered-caller ring	Configures the Nariwake service-registered caller ring cadence.

caller-id alerting dsp-pre-alloc

To statically allocate a digital signal processor (DSP) resource for receiving caller ID information for on-hook (Type 1) caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id alerting dsp-pre-alloc** command in voice-port configuration mode. To disable the command's effect, use the **no** form of this command.

caller-id alerting dsp-pre-alloc

no caller-id alerting dsp-pre-alloc

Syntax Description

This command contains no arguments or keywords.

Command Default

No preallocation of DSP resources

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco MC3810, Cisco 2600 series, and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

The **caller-id alerting dsp-pre-alloc** command may be required on an FXO port if the central office uses line polarity reversal to signal the start of caller-ID information transmission. Preallocating a DSP allows the DSP to listen for caller-ID information continuously without requiring an alerting signal from the central office (CO).

This command is the FXO counterpart to the **caller-id alerting line-reversal** command, which is applied to the Foreign Exchange Station (sending) end of the caller-ID call.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a voice port where caller-ID information is received:

```
voice-port 1/0/1
  cptone US
  caller-id enable
  caller-id alerting line-reversal
  caller-id alerting dsp-pre-alloc
```

Related Commands

Command	Description
caller-id alerting line-reversal	Sets the line-reversal method of caller-ID call alerting.

caller-id alerting line-reversal

To set the line-reversal alerting method for caller-ID information for on-hook (Type 1) caller ID at a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting line-reversal** command in voice-port configuration mode. To disable the command's effect, use the **no** form of this command.

caller-id alerting line-reversal

no caller-id alerting line-reversal

Syntax Description This command has no arguments or keywords.

Command Default No line-reversal alert

Command Modes Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines This command is required only when the telephone device attached to an FXS port requires the line-reversal method to signal the start of a caller-ID transmission. Use it on FXS voice ports that send caller-ID information.

This command is the FXS counterpart to the **caller-id alerting dsp-pre-alloc** command, which is applied to the FXO (receiving) end of the caller-ID call with the line-reversal alerting method.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples The following example configures a voice port from which caller-ID information is sent:

```
voice-port 1/0/1
   cptone US
   station name  A. sample
   station number 4085550111
   caller-id alerting line-reversal
   caller-id alerting dsp-pre-alloc
```

Related Commands

Command	Description
caller-id alerting dsp-pre-alloc	At the receiving end of a line-reversal alerting caller-ID call, preallocates DSPs for caller ID calls.

caller-id alerting pre-ring

To set a 250-millisecond prering alerting method for caller ID information for on-hook (Type 1) caller ID at a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting pre-ring** command in voice-port configuration mode. To disable the command, use the **no** form of this command.

caller-id alerting pre-ring

no caller-id alerting pre-ring

Syntax Description

This command has no arguments or keywords.

Defaults

No prering alert

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco MC3810, Cisco 2600 series, and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command is required only when the telephone device attached to an FXS port requires the prering (immediate ring) method to signal the start of caller ID transmission. Use it on FXS voice ports that send caller ID information. This command allows the FXS port to send a short prering preceding the normal ring cadence. On an FXO port, an incoming prering (immediate ring) is simply counted as a normal ring using the **caller-id alerting ring** command.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
   cptone US
   station name  A. sample
   station number 4085550111
   caller-id alerting pre-ring
```

Related Commands

Command	Description
caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
caller-id alerting ring	Enables caller ID operation and sets an alerting ring type at an FXO or FXS port.

caller-id alerting ring

To set the ring-cycle method for receiving caller ID information for on-hook (Type 1) caller ID at a receiving Foreign Exchange Office (FXO) or a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting ring** command in voice-port configuration mode. To set the command to the default, use the **no** form of this command.

caller-id alerting ring {**1** | **2**}

no caller-id alerting ring

Syntax Description

1	Use this setting if your telephone service provider specifies it to provide caller ID alerting (display) after the first ring at the receiving station. This is the most common setting.
2	Use this setting if your telephone service provider specifies it to provide caller ID alerting (display) after the second ring. This setting is used in Australia, where the caller ID information is sent following two short rings (double-pulse ring).

Command Default

1

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This setting is determined by the Bellcore/Telcordia or ETSI standard that your telephone service provider uses for caller ID. Use it on FXO loop-start and ground-start voice ports where caller ID information arrives and on FXS voice ports from which caller ID information is sent.

This setting must match on the sending and receiving ends of the telephone line connection.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on line.

Examples

The following example configures a voice port where caller ID information is received:

```
voice-port 1/0/1
   cptone US
   caller-id alerting ring 1
```

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
   cptone northamerica
   station name A. sample
   station number 4085550111
   caller-id alerting ring 1
```

Related Commands

Command	Description
caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
caller-id alerting pre-ring	Enables caller ID operation and sets the pre-ring alerting method at an FXS port.

caller-id attenuation

To set the attenuation for caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id attenuation** command in voice-port configuration mode. To set the command to the default, use the **no** form of this command.

caller-id attenuation [*attenuation*]

no caller-id attenuation

Syntax Description

attenuation	(Optional) specifies the attenuation, in decibels (dB). Range is from 0 to 64. The default is 14.

Command Default

The default value is 14 dB, signal level of –14 dBm.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use this setting to specify the attenuation for a caller ID FXO port. If the setting is not used, the attenuation is set to 14 dB, signal level of –14 dBm.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on line.

Examples

The following example configures a voice port where caller ID information is received:

```
voice-port 1/0/1
   cptone US
   caller-id attenuation 0
```

caller-id block

To request the blocking of the display of caller ID information at the far end of a call from calls originated at a Foreign Exchange Station (FXS) port, use the **caller-id block** command in voice-port configuration mode at the originating FXS voice port. To allow the display of caller ID information, use the **no** form of this command.

caller-id block

no caller-id block

Syntax Description

This command has no arguments or keywords.

Command Default

No blocking of caller ID information

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command is used on FXS voice ports that are used to originate on-net telephone calls. This command affects all calls sent to a far-end FXS station from the configured originating FXS station. Calling number and called number are provided in the H.225 setup message for VoIP, through the H.225 Octet 3A field. Calling name information is included in a display information element.

Note Cisco-switched calls using Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) carry calling party information in the Cisco proprietary setup message. For standards-based, point-to-point VoFR (FRF.11) trunks where transparent signaling is applied for FXS-to-FXO calls, only pass-through of in-band automatic number identification (ANI) is supported. ANI information is always unblocked for these communications. Interface technology using transparent channel-associated signaling (CAS) can support only ANI through Feature Group D (in-band MF signaling). The Caller ID feature cannot be used with fixed point-to-point trunk connects created using the **connection trunk** command.

Note Specific hardware is required to provide full support for the caller ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on Cisco.com.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
   cptone US
   station name A. sample
   station number 4085550111
   caller-id block
```

Related Commands

Command	Description
caller-id enable	Enables caller ID operation.

caller-id block (voice register template)

Note Effective with Cisco IOS Release 12.4(11)XJ, the **caller-id block (voice register template)** command is not available in Cisco IOS software.

To enable caller-ID blocking for outbound calls from a specific SIP phone, use the **caller-id block** command in voice register template configuration mode. To disable caller-ID blocking, use the **no** form of this command.

caller-id block

no caller-id block

Syntax Description

This command has no arguments or keywords.

Command Default

Caller ID blocking is disabled.

Command Modes

Voice register template configuration (config-register-temp)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(4)T	Cisco CME 3.4	This command was introduced.
12.4(11)XJ	Cisco Unified CME 4.1	This command was removed.
12.4(15)T	Cisco Unified CME 4.1	This command was removed in Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command sets caller-ID blocking for outbound calls originating from any SIP phone that uses the specified template. This command requests the far-end gateway device to block the display of the calling party information for calls received from the specified SIP phone. This command does not affect the calling party information displayed for inbound calls received by the SIP phone. To apply a template to a SIP phone, use the **template** command in voice register pool configuration mode.

Examples

The following example shows how to enable caller-ID blocking in template 1:

```
Router(config)# voice register template 1
Router(config-register-temp)# caller-id block
```

Related Commands

Command	Description
anonymous block (voice register template)	Enables anonymous call blocking in a SIP phone template.
template (voice register pool)	Applies a template to a SIP phone.
voice register template	Enters voice register template configuration mode and defines a template of common parameters for SIP phones.

caller-id enable

To allow the sending or receiving of caller-ID information, use the **caller-id enable** command in voice-port configuration mode at the sending foreign exchange station (FXS) voice port or the receiving foreign exchange office (FXO) voice port. To disable the sending and receiving of caller-ID information, use the **no** form of this command.

caller-id enable [**type** {**1** | **2**}]

no caller-id enable [**type** {**1** | **2**}]

Syntax Description

type	(Optional) Indicates that the following keyword is a caller-ID type. • **1**—Type I only. Type I transmits the signal when the receiving phone is on hook. • **2**—Type II only. Type II transmits the signal when the receiving phone is off hook, for instance to display the caller ID of an incoming call when the receiving phone is busy (call-waiting caller ID).

Command Default

The sending and receiving of caller-ID information is disabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.3(7)T	The **type 1** and **type 2** keywords were added.

Usage Guidelines

This command applies to FXS voice ports that send caller-ID information and to FXO ports that receive caller-ID information. Calling number and called number are provided in the H.225.0 setup message for VoIP through the H.225.0 Octet 3A field. Calling name information is included in a display information element.

Some users that do not have caller ID type II support on their phones hear noise when type II caller ID is enabled. The **caller-id enable type 1** command allows only type I on the voice port and disables type II, so that the user does not hear this noise.

If this command is used without the optional **type** keyword, both type I and type II caller ID are enabled.

Note The **no** form of this command also clears all other caller-ID configuration settings for the voice port.

Note Cisco-switched calls using Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) carry calling-party information in the Cisco-proprietary setup message. For standards-based, point-to-point VoFR (FRF.11) trunks where transparent signaling is applied for FXS-to-FXO calls, only pass-through of in-band automatic number identification (ANI) is supported. ANI information is always unblocked for these communications. Interface technology using transparent channel-associated signaling (CAS) can support only ANI through Feature Group D (in-band multifrequency signaling). Caller ID cannot be used with fixed point-to-point trunk connections created using the **connection trunk** command.

If the **station name, station number**, or a **caller-id alerting** command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable** command is not necessary.

Note Specific hardware is required to provide full support for the caller-ID features. To determine support for these features in your configuration, review the appropriate hardware documentation and data sheets. This information is available on line.

Examples

The following example configures a Cisco 2600 series or Cisco 3600 series router voice port at which caller-ID information is received:

```
voice-port 1/0/1
 cptone US
 caller-id enable
```

The following example configures a Cisco 2600 series or Cisco 3600 series router voice port from which caller-ID information is sent:

```
voice-port 1/0/1
 cptone northamerica
 station name A. sample
 station number 4085550111
 caller-id enable
```

The following example enables only type I caller ID on port 2/0:

```
voice-port 2/0
 caller-id enable type 1
```

Related Commands

Command	Description
caller-id alerting line-reversal	Enables caller ID operation and sets the line-reversal alerting type at an FXS port.
caller-id alerting pre-ring	Enables caller ID operation and sets the pre-ring alerting method at an FXS port.
caller-id alerting ring	Enables caller ID operation and sets an alerting ring type at an FXO or FXS port.
caller-id block	Disables the sending of caller ID information from an FXS port.
station name	Enables caller ID operation and sets the name sent from an FXS port.
station number	Enables caller ID operation and sets the number sent from an FXS port.

caller-number (dial peer)

To associate a type of ring cadence with a specific caller ID, use the **caller-number** command in dial peer voice configuration mode. To disable the type of ring cadence for a specific caller ID, use the **no** form of this command.

caller-number *number* **ring** *cadence*

no caller-number *number* **ring** *cadence*

Syntax Description

number	Caller ID for which the user wants to set the cadence. Twenty numbers along with their respective cadences may be set for each of the plain old telephone service (POTS) ports.
ring *cadence*	Ring cadence level. The three cadence levels (0, 1, and 2), which differ in duration and cadence, are as follows: • **0**—The ring cadence is 1 second on and 2 seconds off (NTT-defined regular ring). • **1**—The ring cadence is 0.25 seconds on, 0.2 seconds off, 0.25 seconds on, and 2.3 seconds off (NTT-defined nonregular ring). • **2**—The ring cadence is 0.5 seconds on, 0.25 seconds off, 0.25 seconds on, and 2 seconds off (Cisco-defined nonregular ring).

Command Default

The router does not associate any caller ID with a cadence level. Therefore, there is no distinctive ring.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813 routers.

Usage Guidelines

You can enter the **caller-number** command for each POTS port. A maximum of 20 caller IDs can be associated with distinct ring cadences. After 20 numbers per port have been set, you cannot set more numbers (and their ring cadences) for that port until you have removed any of the numbers that have already been set. To remove already-set numbers and their ring cadences, use the **no** form of the **caller-number** command.

The command must be set within each dial peer. Six dial peers are available, you can specify 20 caller IDs per port, for a maximum of 120 caller ID numbers.

Note If you have already subscribed to Nariwake service, the priority goes to the Nariwake caller ID cadence.

To disable distinctive ringing based on a caller ID number, configure the **no caller-number** command. Disabling the ringing removes the specific cadence that has been set for that particular number. If you have set 20 numbers and their ring cadences, you need to set the **no caller-number** command for each of the 20 numbers.

Use the **show running-config** command to check distinctive ringing status.

Examples

The following output examples show that three caller ID numbers and their ring cadences have been set for POTS port 1 and that five caller ID numbers and their ring cadences have been set for POTS port 2:

```
dial-peer voice 1 pots
 destination-pattern 5550102
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 1111111 ring 2
 caller-number 2222222 ring 1
 caller-number 3333333 ring 1

dial-peer voice 2 pots
 destination-pattern 5550110
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 4444444 ring 1
 caller-number 6666666 ring 2
 caller-number 7777777 ring 0
 caller-number 8888888 ring 1
 caller-number 9999999 ring 2
```

Related Commands

Command	Description
call-waiting	Enables call waiting.
volume	Configures the receiver volume level in the router.

calling-info pstn-to-sip

To specify calling information treatment for public switched telephone network (PSTN) to Session Initiation Protocol (SIP) calls, use the **calling-info pstn-to-sip** command in SIP user agent configuration mode. To disable calling information treatment for PSTN-to-SIP calls, use the **no** form of this command.

calling-info pstn-to-sip {**unscreened discard** | {**from** | **remote-party-id** | **asserted-id** {**name set** *name* | **number set** *number*}}}

no calling-info pstn-to-sip

Syntax Description

unscreened discard	(Optional) Specifies that the calling name and number be discarded.
from name set *name*	(Optional) Specifies that the display-name of the From header is unconditionally set to the configured ASCII string in the forwarded INVITE message.
from number set *number*	(Optional) Specifies that the user part of the From header is unconditionally set to the configured ASCII string in the forwarded INVITE message.
remote-party-id name set *name*	(Optional) Specifies that the display-name of the Remote-Party-ID header is unconditionally set to the configured ASCII string in the forwarded INVITE message.
remote-party-id number set *number*	(Optional) Specifies that the user part of the Remote-Party-ID header is unconditionally set to the configured ASCII string in the forwarded INVITE message.
asserted-id name set *name*	(Optional) Specifies that the display-name in the Asserted-ID header is unconditionally set to the configured ASCII string in the forwarded INVITE message.
asserted-id number set *number*	(Optional) Specifies that the user part in the Asserted-ID header is unconditionally set to the configured ASCII string in the forwarded INVITE message.

Command Default

This command is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(15)T	The **asserted-id** keyword was added.

Usage Guidelines

When a call exits the gateway, the **calling-info pstn-to-sip** treatments are applied.

Examples

The following example enables calling information treatment for PSTN-to-SIP calls and sets the company name and number:

```
Router(config-sip-ua)# calling-info pstn-to-sip from name set CompanyA
Router(config-sip-ua)# calling-info pstn-to-sip from number set 5550101
Router(config-sip-ua)# exit
Router(config)# exit

Router# show running-config
Building configuration...

.
.
.
!
sip-ua
 calling-info pstn-to-sip from name set CompanyA
 calling-info pstn-to-sip from number set 5550101
 no remote-party-id
!
.
.
.
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either P-Asserted-Identity (PAI) or P-Preferred-Identity (PPI) privacy headers in outgoing SIP requests or response messages.
calling-info sip-to-pstn	Specifies calling information treatment for SIP-to-PSTN calls.
debug ccsip events	Enables tracing of SIP SPI events.
debug ccsip messages	Enables tracing SIP messages exchanged between the SIP UA client and the access server.
debug isdn q931	Displays call setup and teardown of ISDN connections.
debug voice ccapi error	Enables tracing error logs in the call control API.
debug voip ccapi in out	Enables tracing the execution path through the call control API.

calling-info sip-to-pstn

To specify calling information treatment for Session Initiation Protocol (SIP) to public switched telephone network (PSTN) calls, use the **calling-info sip-to-pstn** command in SIP user agent configuration mode. To disable calling information treatment for SIP-to-PSTN calls, use the **no** form of this command.

calling-info sip-to-pstn {**unscreened discard** | **name set** *name* | **number set** *number*}

no calling-info sip-to-pstn

Syntax Description

unscreened *discard*	(Optional) Specifies that the calling name and number be discarded.
name set *name*	(Optional) Specifies that the calling name be unconditionally set to the configured ASCII string in the forwarded Setup mesage.
number set *number*	(Optional) Specifies that the calling number be unconditionally set to the configured ASCII string in the forwarded Setup message.

Command Default

This command is disabled.

Command Modes

SIP user agent configuration (config-sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

When a call enters the gateway, the **calling-info sip-to-pstn** treatments are applied.

Examples

The following example enables calling information treatment for SIP-to-PSTN calls and sets the company name to CompanyA and the number to 5550100:

```
Router(config-sip-ua)# calling-info sip-to-pstn name set CompanyA
Router(config-sip-ua)# calling-info sip-to-pstn number set 5550100
Router(config-sip-ua)# exit
Router(config)# exit
```

```
Router# show running-config
Building configuration...

.
.
.
!
sip-ua
 calling-info sip-to-pstn name set CompanyA
     calling-info sip-to-pstn number set 5550100
!
.
.
.
```

Related Commands

Command	Description
debug ccsip events	Enables tracing of SIP SPI events.
debug ccsip messages	Enables SIP SPI message tracing.
debug isdn q931	Displays call setup and teardown of ISDN connections.
debug voip ccapi in out	Enables tracing the execution path through the call control API.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.

calling-number outbound

To specify automatic number identification (ANI) to be sent out when T1-channel-associated signaling (T1-CAS) Feature Group D-Exchange Access North American (FGD-EANA) is configured as the signaling type, use the **calling-number outbound** command in dial peer or voice-port configuration mode. To disable this command, use **no** form of this command.

calling-number outbound {**range** *string1 string2* | **sequence** *string1*... *string5* | **null**}

no calling-number outbound {**range** *string1 string2* | **sequence** *string1*... *string5* | **null**}

Syntax Description

range	Generates the sequence of ANI by rotating through the specified range (*string1* to *string2*).
sequence	Configures a sequence of discrete strings (*string1*... *string5*) to be passed out as ANI for successive calls using the peer **Note** The ellipses (**...**) is entered as shown above.
null	Suppresses ANI. If used, no ANI is passed when this dial peer is selected.
string#...	Valid E.164 telephone number strings. Strings must be of equal length and cannot be more than 32 digits long.

Command Default

No outbound calling number is specified.

Command Modes

Dial peer configuration (config-dial-peer)
Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.

Usage Guidelines

This command is effective only for FGD-EANA signaling.

Examples

Use the **calling-number outbound** command to enable or disable the passing of ANI on a T1-CAS FGD-EANA configured T1 interface for outgoing calls. Syntax for this command is the same for both voice-port mode and dial peer mode. Examples are given for both modes.

calling-number outbound Range

```
calling-number outbound range string1 string2
```

The values *string1* and *string2* are valid E.164 telephone number strings. Both strings must be of the same length and cannot be more than 32 digits long. Only the last four digits are used for specifying the range (*string1* to *string2*) and for generating the sequence of ANI by rotating through the range until *string2* is reached and then starting from *string1* again. If strings are fewer than four digits in length, then entire strings are used.

ANI is generated by using the 408555 prefix and by rotating through 0100 to 0101 for each call using this peer.

Dial peer configuration mode:

```
dial-peer voice 1 pots
 calling-number outbound range 4085550100 4085550101
 calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
 calling-number outbound range 4085550100 4085550105
 Calling Number Outbound is effective only for fgd_eana signaling
```

calling-number outbound Sequence

```
calling-number outbound sequence string1 string2 string3
string4 string5
```

This option configures a sequence of discrete strings (*string1... string5*) to be passed out as ANI for successive calls using the peer. The limit is five strings. All strings must be valid E.164 numbers, up to 32 digits in length.

Dial peer configuration mode:

```
dial-peer voice 1 pots
 calling-number outbound sequence 6000 6006 4000 5000 5025
 Calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
 calling-number outbound sequence 6000 6006 4000 5000 5025
 Calling Number Outbound is effective only for fgd_eana signaling
```

calling-number outbound Null

```
calling-number outbound null
```

This option suppresses ANI. If used, no ANI is passed when this dial peer is selected.

Dial peer configuration mode:

```
dial-peer voice 1 pots
 calling-number outbound null
 Calling Number Outbound is effective only for fgd_eana signaling
```

Voice-port configuration mode:

```
voice-port 1:D
 calling-number outbound null
 Calling Number Outbound is effective only for fgd_eana signaling
```

Related Commands

Command	Description
info-digits string1	Configures two information digits to be prepended to the ANI string.

cancel-call-waiting

To define a feature code for a Feature Access Code (FAC) to enable the Cancel Call Waiting feature, use the **cancel-call-waiting** command in STC application feature access-code configuration mode. To reset the feature code to its default, use the **no** form of this command.

cancel-call-waiting *keypad-character*

no cancel-call-waiting

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 8. The string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default Feature code for Cancel Call Waiting is 8.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines This command changes the default value of the feature code for Cancel Call Waiting (8).

If you attempt to configure this command with a value that is already configured for another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

If you attempt to configure this command with a value that precludes or is precluded by another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for cancel call waiting. With this configuration, a phone user must press **9 on the phone keypad to cancel call waiting.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# cancel-call-waiting **9
```

Related Commands

Command	Description
prefix (stcapp-fac)	Defines the prefix for FACs.
show stcapp feature codes	Displays all FACs.

capacity update interval (dial peer)

To change the capacity update for prefixes associated with this dial peer, use the **capacity update interval** command in dial peer configuration mode. To return to the default, use the **no** form of this command.

capacity update interval *seconds*

no capacity update interval *seconds*

Syntax Description

seconds	Interval, in seconds, between the sending of periodic capacity updates. This can be a number in the range 10 to 1000. The default value is 25 seconds.

Command Default

25 seconds

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The update interval should be set depending how many updates that are sent. Updates are sent more often when more calls are coming in, which can lead to data getting out of synchrony. If the interval is too short for the number of updates, the location server can be overwhelmed.

If a dial peer gets too much traffic, set the *seconds* argument to a higher value.

Examples

The following example shows that POTS dial peer 10 is having the capacity update occur every 35 seconds:

```
Router(config)# dial-peer voice 10 pots
Router(config-dial-peer)# capacity update interval 35
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

capacity update interval (trunk group)

To change the capacity update for carriers or trunk groups, use the **capacity update interval** command in trunk group configuration mode. To return to the default, use the **no** form of this command.

capacity {**carrier** | **trunk-group**} **update interval** *seconds*

no capacity {**carrier** | **trunk-group**}

Syntax Description

carrier	Carrier capacity.
trunk-group	Trunk group capacity.
seconds	Interval, in seconds, between the sending of periodic capacity updates. This can be a number in the range 10 to 1000. The default value is 25 seconds.

Command Default 25 seconds

Command Modes Trunk group configuration (config-trunkgroup)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines The update interval should be set depending how many updates that are sent. Updates are sent more often when more calls are coming in, which can lead to data getting out of synchrony. If the interval is too short for the number of updates, the location server can be overwhelmed.

If a dial peer gets too much traffic, set the *seconds* argument to a higher value.

Examples The following example sets the capacity update for trunk group 101 to occur every 45 seconds:

```
Router(config)# trunk group 101
Router(config-trunkgroup)# capacity trunk-group update interval 45
```

Related Commands

Command	Description
trunk group	Defines the trunk group and enters trunk group configuration mode.

cap-list vfc

To add a voice codec overlay file to the capability file list, use the **cap-list vfc** command in global configuration mode. To disable a particular codec overlay file that has been added to the capability list, use the **no** form of this command.

cap-list *filename* **vfc** *slot-number*

no cap-list *filename* **vfc** *slot-number*

Syntax Description

filename	Identifies the codec file stored in voice feature card (VFC) flash memory.
slot-number	Identifies the slot where the VFC is installed. Range is 0 to 2. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3NA	This command was introduced on the Cisco AS5300.

Usage Guidelines

When VCWare is unbundled, it automatically adds DSPWare to flash memory, creates both the capability and default file lists, and populates these lists with the default files for the particular version of VCWare. The capability list defines the available voice codecs for H.323 capability negotiation. Use the **cap-list vfc** command to add the indicated voice codec overlay file (defined by *filename*) to the capability file list in flash memory.

Examples

The following example adds the following codec to the list included in flash memory:

```
config terminal
 cap-list cdc-g711-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
default-file vfc	Specifies an additional (or different) file from the ones in the default file list and stored in VFC Flash memory.

card type (T1-E1)

To configure a T1 or E1 card type, use the **card type** command in global configuration mode. To deselect the card type on non-SPA platforms, use the **no** form of this command. The **no** form of this command is not available on the SPA platforms.

card type {**t1** | **e1**} *slot* [*bay*]

no card type {**t1** | **e1**} *slot* [*bay*]

Channelized T/E1 Shared Port Adapters

card type {**t1** | **e1**} *slot subslot*

Syntax Description

t1	Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding.
e1	Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
bay	(Optional) Card interface bay number in a slot (route switch processor [RSP] platform only). This option is not available on other platforms.
subslot	(Channelized T/E1 Shared Port Adapters Only) Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1) and support was added for Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 platforms.
12.2S	This command was integrated into Cisco IOS Release 12.2S.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Changes made using this command on non-SPA platforms, do not take effect unless the **reload** command is used or the router is rebooted.

Channelized T1/E1 Shared Port Adapters

There is no card type when the SPA is inserted for first time. The user must configure this command before they can configure individual ports.

The **no** form of this command is not available on the SPA platforms. To change an existing card type on SPA platforms, perform the following steps:

1. Remove the SPA from its subslot.
2. Save the configuration.
3. Reboot the router.
4. Insert the new SPA into the subslot.
5. Configure the new card using this command.

Examples

The following example configures T1 data transmission on slot 1 of the router:

```
Router(config)# card type t1 1
```

The following example configures all ports of an 8-Port Channelized T1/E1 SPA, seated in slot 5, subslot 2, in T1 mode:

```
Router(config)# card type t1 5 2
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
reload	Reloads the operating system.
show controller	Displays the controller state that is specific to controller hardware
show interface serial	Displays the serial interface type and other information.

card type (T3-E3)

To configure a T3 or E3 card type, use the **card type** command in global configuration mode. To deselect the card type, use the **no** form of this comand. The **no** form of this command is not supported on the 2-Port and 4-Port Clear Channel T3/E3 SPA on Cisco 12000 series routers.

T3 or E3 Controllers

card type {**t3** | **e3**} *slot*

no card type {**t3** | **e3**} *slot*

Clear Channel T3/E3 Shared Port Adapters

card type {**t3** | **e3**} *slot subslot*

no card type {**t3** | **e3**} *slot subslot*

Clear Channel T3/E3 Shared Port Adapters on Cisco 12000 Series Routers

card type {**t3** | **e3**} *slot subslot*

Syntax Description

t3	Specifies T3 connectivity of 44210 kbps through the network, using B8ZS coding.
e3	Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34010 kbps.
slot	Slot number of the interface.
subslot	(Clear Channel T3/E3 Shared Port Adapters Only) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Release	Modification
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1) and support was added for Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 platforms.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Usage guidelines vary slightly from platform to platform as follows:

T3 or E3 Controllers

Once a card type is issued, you enter the **no card type** command and then another **card type** command to configure a new card type. You must save the configuration to the NVRAM and reboot the router in order for the new configuration to take effect.

When the router comes up, the software comes up with the new card type. Note that the software will reject the configuration associated with the old controller and old interface. You must configure the new controller and serial interface and save it.

Clear Channel T3/E3 Shared Port Adapters

To change all the SPA ports from T3 to E3, or vice versa, you enter the **no card type** command and then another **card type** command to configure a new card type.

When the router comes up, the software comes up with the new card type. Note that the software will reject the configuration associated with the old controller and old interface. You must configure the new controller and serial interface and save it.

Clear Channel T3/E3 Shared Port Adapters on Cisco 12000 Series Routers

The **no** form of this command is not available on the 2-Port and 4-Port Clear Channel T3/E3 SPA on Cisco 12000 series routers. To change an existing card type on Cisco 12000 series routers, perform the following steps:

1. Remove the SPA from its subslot.
2. Save the configuration.
3. Reboot the router.
4. Insert the new SPA into the subslot.
5. Configure the new card using this command.

Examples

The following example shows T3 data transmission configured in slot 1:

```
Router(config)# card type t3 1
```

The following example configures all ports of 2-Port and 4-Port Clear Channel T3/E3 SPA, seated in slot 5, subslot 2, in T3 mode:

```
Router(config)# card type t3 5 2
```

Related Commands

Command	Description
controller	Configures a T3 or E3 controller and enters controller configuration mode.
reload	Reloads the operating system.
show interface serial	Displays the serial interface type and other information.

carrier-id (dial peer)

To specify the carrier associated with a VoIP call in a dial peer, use the **carrier-id** command in dial peer configuration mode. To delete the source carrier ID, use the **no** form of this command.

carrier-id {**source** | **target**} *name*

no carrier-id {**source** | **target**} *name*

Syntax Description

source	Indicates the carrier that the dial peer uses as a matching key for inbound dial-peer matching.
target	Indicates the carrier that the dial peer uses as a matching key for outbound dial-peer matching.
name	Specifies the ID of the carrier to use for the call. Valid carrier IDs contain a maximum of 127 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

A Gatekeeper Transaction Message Protocol (GKTMP) route server-based application at the terminating gateway uses the source carrier ID to select a target carrier that routes the call over a plain old telephone service (POTS) line.

The terminating gateway uses the target carrier ID to select a dial peer for routing the call over a POTS line.

For IP-to-IP calls, the **carrier-id** command alone is not an oubound dialpeer match criterion.

Examples

The following example indicates that dial peer 112 should use carrier ID “east17” for outbound dial-peer matching in the terminating gateway:

```
Router(config)# dial-peer voice 112 pots
Router(config-dial-peer)# carrier-id target east17
```

The following example indicates that dial peer 111 should use carrier ID “beta23” for inbound dial-peer matching in the terminating gateway:

```
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# carrier-id source beta23
```

Related Commands

Command	Description
translation-profile (dial peer)	Associates a translation profile with a dial peer.
trunkgroup (dial peer)	Assigns a trunk group to a source IP group or dial peer for trunk group label routing.

carrier-id (global)

To set the carrier ID for trunk groups when a local carrier ID is not configured, use the **carrier-id** command in global configuration mode. To disable the carrier ID, use the **no** form of this command.

carrier-id *name* [**cic**]

no carrier-id *name* [**cic**]

Syntax Description

name	Identifier for the carrier ID. Must be four-digit numeric carrier identification code to be advertised as a TRIP carrier family but can be alphanumeric if used otherwise.
cic	(Optional) Specifies that the carrier ID is a circuit identification code (CIC).

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

To advertise the carrier as a TRIP carrier family, the **cic** keyword must be used. When the **cic** keyword is used, only numeric values can be accepted for the *name* value. If the **cic** keyword is not used, the *name* value can be alphanumeric but is not advertised to TRIP location servers.

Examples

The following example shows a carrier ID using the circuit identification code:

```
Router(config)# carrier-id 1234 cic
```

Related Commands

Command	Description
carrier-id (trunk group)	Configures the carrier ID locally on the trunk group.

carrier-id (trunk group)

To specify the carrier associated with a trunk group, use the **carrier-id** command in trunk group configuration mode. To delete the source carrier ID, use the **no** form of this command.

carrier-id *name* [**cic**]

no carrier-id *name* [**cic**]

Syntax Description

name	The ID of the carrier to use for the call. Valid carrier IDs contain a maximum of 127 alphanumeric characters. To be advertised as a TRIP carrier family, this must be set to a four-digit numeric carrier identification code.
cic	(Optional) Specifies that the carrier ID is a circuit identification code.

Command Default No default behavior or values

Command Modes Trunk group configuration (config-trunkgroup)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(1)	The **cic** keyword was added.

Usage Guidelines In a network, calls are routed over incoming trunk groups and outgoing trunk groups. The *name* arguments identifies the carrier that handles the calls for a specific trunk group. In some cases, the same trunk group may be used to carry both incoming calls and outgoing calls.

The carrier ID configured locally on the trunk group supersedes the globally configured carrier ID.

To advertise the carrier as a TRIP carrier family, the **cic** keyword must be used. When **cic** is used, only numeric values can be accepted for the *name* value. If **cic** is not used, the *name* value can be alphanumeric but is not advertised to TRIP location servers.

Examples The following example indicates that carrier “alpha1” carries calls for trunk group 5:

```
Router(config)# trunk group 5
Router(config-trunk-group)# carrier-id alpha1
```

The following example shows that the carrier with circuit identification code 1234 carries calls for trunk group 101. This trunk group can carry TRIP advertisements.

```
Router(config)# trunk group 101
Router(config-trunk-group)# carrier-id 1234 cic
```

Related Commands

Command	Description
carrier-id (global)	Configures the carrier ID globally for all trunk groups.
translation-profile (trunk group)	Associates a translation profile with a trunk group.
trunk group	Initiates the definition of a trunk group.

carrier-id (voice source group)

To specify the carrier associated with a VoIP call, use the **carrier-id** command in voice source group configuration mode. To delete the source carrier ID, use the **no** form of this command.

carrier-id {**source** | **target**} *name*

no carrier-id {**source** | **target**} *name*

Syntax Description

source	Indicates the carrier ID associated with an incoming VoIP call at the terminating gateway.
target	Indicates the carrier ID used by the terminating gateway to match an outbound dial peer.
name	The ID of the carrier to use for the call. Valid carrier IDs contain a maximum of 127 alphanumeric characters.

Command Default No default behavior or values

Command Modes Voice source group configuration (cfg-source-grp)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines A Gatekeeper Transaction Message Protocol (GKTMP) server application at the terminating gateway uses the source carrier ID to select a target carrier that routes the call over a plain old telephone service (POTS) line. The terminating gateway uses the target carrier ID to select a dial peer for routing the call over a POTS line.

Note If an incoming H.323 VoIP call matches a source IP group that has a target carrier ID, the source IP group's target carrier ID overrides the VoIP call's H.323 setup message.

Examples The following example indicates that voice source IP group "group1" should use carrier ID named "source3" for incoming VoIP calls and carrier ID named "target17" for outbound dial-peer matching in the terminating gateway:

```
Router(config)# voice source-group group1
Router(cfg-source-grp)# carrier-id source source3
Router(cfg-source-grp)# carrier-id target target17
```

Related Commands

Command	Description
voice source-group	Initiates the definition of a source IP group.

cause-code

To represent internal failures with former and nonstandard H.323 or Session Initiation Protocol (SIP) cause codes, use the **cause-code** command in voice service VoIP configuration mode. To use standard cause-code categories, use the **no** form of this command.

cause-code legacy

no cause-code legacy

Syntax Description

legacy	Sets the internal cause code to the former and nonstandard set of H.323 and SIP values.

Command Default

The default for SIP and H.323 is to use standard cause-code categories, so the command is disabled.

Command Modes

Voice service VoIP configuration (config-voi-srv)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command is used for backward compatibility purposes.

Examples

The following example sets the internal cause codes to the former and nonstandard set of SIP and H.323 values for backward compatibility:

```
Router(config)# voice service voip
Router(config-voi-srv)# cause-code legacy
```

Related Commands

Command	Description
show call history voice	Displays the call history table for voice calls.

cbarge

To enable idle phones to join an active call on a shared line on a Foreign Exchange Station (FXS) port by going offhook, use the **cbarge** command in supplementary-service voice-port configuration mode. To return to the command default, use the **no** form of this command.

cbarge

no cbarge

Syntax Description

This command has no arguments or keywords.

Command Default

cBarge is disabled and idle phones are unable to join an active call on a shared line.

Command Modes

Supplementary-service voice-port configuration mode (config-stcapp-suppl-serv-port)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **cbarge** command to allow one idle IP or analog phone that is connected to the same FXS port to automatically join an active call on the shared line by going offhook.

The **hold-resume** command must be configured on each port before the **cbarge** command is configured.

Only one analog phone is allowed to join an active call.

Examples

The following example shows how to enable idle phones to join active calls on ports 2/2, 2/3, and 2/4 on a Cisco VG224:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/2
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# cbarge
Router(config-stcapp-suppl-serv)# port 2/3
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# cbarge
Router(config-stcapp-suppl-serv)# port 2/4
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# cbarge
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
hold-resume	Turns the STCAPP supplementary-service features on and off using hookflash.
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

ccm-manager application redundant-link port

To configure the port number for the redundant link application, use the **ccm-manager application redundant-link port** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ccm-manager application redundant-link port *number*

no ccm-manager application redundant-link port

Syntax Description

port *number*	Port number for the transport protocol. The protocol may be User Data Protocol (UDP), Reliable User Datagram Protocol (RDUP), or TCP. Range is from 0 to 65535, and the specified value must not be a well-known reserved port number such as 1023. The default is 2428.

Command Default

Port number: 2428

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (VG200).
12.2(2)XA	The command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

Use this command only when defining an application-specific port other than the default.

Examples

In the following example, the port number of the redundant link application is 2429:

```
ccm-manager application redundant-link port 2429
```

Related Commands

Command	Description
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager is used if it becomes available again while a backup Cisco CallManager is being used.

ccm-manager config

To specify the TFTP server from which the Media Gateway Control Protocol (MGCP) gateway downloads Cisco Unified Communications Manager (Cisco UCM) Extensible Markup Language (XML) configuration files and to enable the download of the configuration, use the **ccm-manager config** command in global configuration mode. To disable the dial-peer and server configurations, use the **no** form of this command.

ccm-manager config [**dialpeer-prefix** *prefix* | **server** {*ip-address* | *name*}]

no ccm-manager config [**dialpeer-prefix** *prefix* | **server**]

Syntax Description

dialpeer-prefix *prefix*	(Optional) Specifies the prefix to use for autogenerated dial peers. Range is 1 to 2147483647. The default is 999. **Note** When manually adding a dial peers prefix, select a prefix number other than the default.
server {*ip-address* | *name*}	(Optional) Specifies the IP address or logical name of the TFTP server from which the XML configuration files are downloaded. The arguments are as follows: • *ip-address*—IP address of the TFTP server from which to download the XML configuration files to the local MGCP voice gateway. • *name*—Logical (symbolic) name of the TFTP server from which to download XML configuration files to the local MGCP voice gateway.

Command Default

The configuration download feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XN	This command was introduced and implemented on the Cisco 2600 series, Cisco 3600 series, and the Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco IAD2420 series.

Usage Guidelines

The **ccm-manager config** command is required to enable the download of Cisco UCM XML configuration files. If you separate the MGCP and H.323 dial peers under different dial-peer tags, ensure that the MGCP dial peers are configured before the H.323 dial peers. Direct-inward-dial (DID) is required for E1 PRI dial peers.

Note To keep manually added dial peers from being deleted from the running configuration when Cisco UCM downloads the configuration to the gateway, use a dial peer-prefix value other than the default (999).

Do not delete the POTS dial peer created by the automatic download process. However, if a dial peer has been deleted, you can restore the deleted dial peer by entering the following commands to repeat the download of the configuration file:

```
no mgcp
no ccm-manager config
ccm-manager config
mgcp
```

After you enter these commands, use the **show ccm-manager config-download** command to display the the configuration file downloaded from the TFTP server via the interface specified. The following is an example of the output:

```
Loading sample.cnf.xml from 9.13.22.100 (via GigabitEthernet0/0): !
[OK - 12759 bytes]
```

Examples

The following example shows how to enable the automatic download of configuration files:

```
ccm-manager config
```

In the following example, the IP address of the TFTP server from which a configuration file is downloaded is identified:

```
ccm-manager config server 10.10.0.21
```

Related Commands

Command	Description
debug ccm-manager config-download	Displays dialog during configuration download from the Cisco UCM to the gateway.
show ccm-manager config-download	Displays whether the Cisco UCM configuration is enabled.

Usage Guidelines

The **ccm-manager config** command is required to enable the download of Cisco UCM XML configuration files. If you separate the MGCP and H.323 dial peers under different dial-peer tags, ensure that the MGCP dial peers are configured before the H.323 dial peers. Direct-inward-dial (DID) is required for E1 PRI dial peers.

Note To keep manually added dial peers from being deleted from the running configuration when Cisco UCM downloads the configuration to the gateway, use a dial peer-prefix value other than the default (999).

Do not delete the POTS dial peer created by the automatic download process. However, if a dial peer *has* been deleted, you can restore the deleted dial peer by entering the following commands to repeat the download of the configuration file:

```
no mgcp
no ccm-manager config
ccm-manager config
mgcp
```

After you enter these commands, use the **show ccm-manager config-download** command to display the the configuration file downloaded from the TFTP server via the interface specified. The following is an example of the output:

```
Loading sample.cnf.xml from 9.13.22.100 (via GigabitEthernet0/0): !
[OK - 12759 bytes]
```

Examples

The following example shows how to enable the automatic download of configuration files:

```
ccm-manager config
```

In the following example, the IP address of the TFTP server from which a configuration file is downloaded is identified:

```
ccm-manager config server 10.10.0.21
```

Related Commands

Command	Description
debug ccm-manager config-download	Displays dialog during configuration download from the Cisco UCM to the gateway.
show ccm-manager config-download	Displays whether the Cisco UCM configuration is enabled.

ccm-manager download-tones

To configure a Cisco IOS gateway to download a XML configuration file that contains custom tone information from a TFTP server at the time of gateway registration, use the **ccm-manager download-tones** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ccm-manager download-tones

no ccm-manager download-tones

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco CallManager download tones are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows a Cisco IOS gateway being configured to download an XML configuration file that contains custom tone information from a TFTP server:

```
Router(config)# ccm-manager download-tones
```

Related Commands

Command	Description
cptone	Specifies a regional voice-interface-related tone, ring, and cadence setting.
debug ccm-manager	Displays debugging of Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers and their current status and availability.

ccm-manager fallback-mgcp

To enable the gateway fallback feature and allow a Media Gateway Control Protocol (MGCP) voice gateway to provide call processing services when Cisco CallManager is unavailable, use the **ccm-manager fallback-mgcp** command in global configuration mode. To disable fallback on the MGCP voice gateway, use the **no** form of this command.

ccm-manager fallback-mgcp

no ccm-manager fallback-mgcp

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway fallback feature is enabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XN	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on Cisco IAD2420 series.
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ.
12.3(2)T	This command was implemented on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx.

Usage Guidelines

This command causes the gateway to fall back and provide call processing services if connectivity is lost between the gateway and all Cisco CallManager servers. The mode and timing are set by default.

Examples

The following example enables fallback:

```
Router(config)# ccm-manager fallback-mgcp
```

Related Commands

Related Command	Purpose
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.

ccm-manager fax protocol

To enable fax-relay protocol for endpoints on a gateway, use the **ccm-manager fax protocol** command in global configuration mode. To disable fax-relay protocol, use the **no** form of this command.

ccm-manager fax protocol cisco

no ccm-manager fax protocol cisco

Syntax Description		
	cisco	Cisco-proprietary fax-relay protocol. This is the only choice.

Command Default Cisco-proprietary fax-relay protocol is enabled by default.

Command Default Fax relay is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(9)T	This command was introduced.

Usage Guidelines Use the **no** form of this command to disable fax relay.

Because fax relay is enabled by default, the **show running-config** command does not explicitly show it to be enabled.

Fax over IP enables interoperability of traditional analog fax machines with IP telephony networks. In its original form, fax data is digital. For transmission across a traditional public switched telephone network (PSTN), it is converted to analog form. For transmission across the IP (packet) network, it is reconverted to digital form, and then, at the destination fax machine, converted again to analog form.

Most Cisco voice gateways support two methods of transmitting fax traffic across the IP network:

- Cisco fax relay—The gateway terminates the T.30 fax signaling. This is the preferred method.
- Fax pass-through—The gateway does not distinguish a fax call from a voice call. All Cisco voice gateways support fax pass-through.

Examples The following example configures a Media Gateway Control Protocol (MGCP) gateway for Cisco fax relay:

```
Router(config)# ccm-manager fax protocol cisco
Router(config)# mgcp fax t38 inhibit
```

The following example configures an MGCP gateway for fax pass-through:

```
Router(config)# ccm-manager fax protocol cisco
Router(config)# mgcp modem passthrough voip mode nse
Router(config)# mgcp modem passthrough voip codec g711ulaw
```

Related Commands

Command	Description
debug ccm-manager	Displays debugging of Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers and their current status and availability.
show running-config	Displays the contents of the currently running configuration file.

ccm-manager mgcp

To enable the gateway to communicate with Cisco CallManager through the Media Gateway Control Protocol (MGCP) and to supply redundant control agent services, use the **ccm-manager mgcp** command in global configuration mode. To disable communication with Cisco CallManager and redundant control agent services, use the **no** form of this command.

ccm-manager mgcp [**codec-all**]

no ccm-manager mgcp [**codec-all**]

Syntax Description

codec-all	(Optional) Enables all codec on the gateway for the Cisco CallManager.

Command Default

Cisco CallManager does not communicate with the gateway through MGCP.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 on the Cisco VG200.
12.2(2)XA	The command was integrated into Cisco IOS Release 12.2(2)XA and implemented on the Cisco 2600 series and Cisco 3600 series.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, 3600 series, and Cisco VG200.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and was implemented on the Cisco IAD2420 series routers.
12.2(11)YU	This command was integrated into Cisco IOS Release 12.2(11)YU and implemented on the Cisco 1760 gateway.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **codec-all** keyword was added.

Usage Guidelines

This command enables the gateway to communicate with Cisco CallManager through MGCP. This command also enables control agent redundancy when a backup Cisco CallManager server is available.

Examples

In the following example, support for Cisco CallManager and redundancy is enabled within MGCP:

```
Router# configure terminal
Router(config)# ccm-manager mgcp
```

Related Commands

Command	Description
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager is used if it becomes available again while a backup Cisco CallManager is being used.
mgcp	Enables Media Gateway Control Protocol mode.

ccm-manager music-on-hold

To enable the multicast music-on-hold (MOH) feature on a voice gateway, use the **ccm-manager music-on-hold** command in global configuration mode. To disable the MOH feature, use the **no** form of this command.

ccm-manager music-on-hold

no ccm-manager music-on-hold

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(2)XN	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD 2420 series routers.

Examples The following example shows multicast MOH configured for a MGCP voice gateway:

```
mgcp call-agent 10.0.0.21 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000
mgcp modem passthrough voip mode cisco
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
call rsvp-sync
!
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.0.0.21
!
```

Related Commands

Command	Description
ccm-manager music-on-hold bind	Enables the multicast MOH feature on a voice gateways.
debug ccm-manager music-on-hold	Displays debugging information for MOH.
show ccm-manager music-on-hold	Displays MOH information.

ccm-manager music-on-hold bind

To bind the multicast music-on-hold (MOH) feature to an interface type, use the **ccm-manager music-on-hold bind** command in global configuration mode. To unbind the MOH feature on the interface type, use the **no** form of this command.

ccm-manager music-on-hold bind *type slot/port*

no ccm-manager music-on-hold bind *type slot/port*

Syntax Description

type	Interface type to which the MOH feature is bound. The options follow: • **async**—Asynchronous interface • **bvi**—Bridge-Group Virtual Interface • **ctunnel**—CTunnel interface • **dialer**—Dialer interface • **ethernet**—IEEE 802.3 • **lex**—Lex interface • **loopback**—Loopback interface • **mfr**—Multilink Frame Relay bundle interface • **multilink**—Multilink interface • **null**—Null interface • **serial**—Serial interface • **tunnel**—Tunnel interface • **vif**—PGM Multicast Host interface • **virtual-FrameRelay**—Virtual Frame Relay interface • **virtual-Template**—Virtual template interface • **virtual-TokenRing**—Virtual Token Ring
slot/port	Number of the slot being configured. See the appropriate hardware manual for slot and port information.

Command Default

This command is disabled by default, so the MOH feature is not bound to an interface type.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **ccm-manager music-on-hold bind** command to bind the multicast music-on-hold (MOH) feature to an interface type. Dynamic configuration of multicast MOH bind is not supported.

Examples

The following example shows multicast MOH bound to serial interface 0/0:

```
ccm-manager music-on-hold bind serial 0/0
```

Related Commands

Command	Description
ccm-manager music-on-hold	Enables the MOH feature.
debug ccm-manager music-on-hold	Displays debugging information for MOH.
show ccm-manager music-on-hold	Displays MOH information.

ccm-manager redundant-host

To configure the IP address or the Domain Name System (DNS) name of one or two backup Cisco CallManager servers, use the **ccm-manager redundant-host** command in global configuration mode. To disable the use of backup Cisco CallManager servers as call agents, use the **no** form of this command.

ccm-manager redundant-host {*ip-address* | *dns-name*} [*ip-address* | *dns-name*]

no ccm-manager redundant-host {*ip-address* | *dns-name*} [*ip-address* | *dns-name*]

Syntax Description

ip-address	IP address of the backup Cisco CallManager server.
dns-name	DNS name of the backup Cisco CallManager server.

Command Default

If you do not configure a backup Cisco CallManager, the redundancy is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced with Cisco CallManager Version 3.0 on the Cisco Voice Gateway 200 (VG200).
12.2(2)XA	The command was implemented on the Cisco 2600 series and Cisco 3600 series. The *dns-name* argument was added.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, 3600 series, and the Cisco VG200.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series routers.

Usage Guidelines

The list of IP addresses or DNS names is an ordered and prioritized list. The Cisco CallManager server that was defined with the **mgcp call-agent** command has the highest priority—it is the primary Cisco CallManager server. The gateway selects a Cisco CallManager server on the basis of the order of its appearance in this list.

Examples

In the following example, the IP address 10.0.0.50 is configured as the backup Cisco CallManager :

```
ccm-manager redundant-host 10.0.0.50
```

Related Commands

Command	Description
ccm-manager application	Configures the port number for the redundant link application.
ccm-manager switchback	Configures the switchback mode that determines when the primary Cisco CallManager is used if it becomes available again while a backup Cisco CallManager is being used.
ccm-manager switchover-to-backup	Redirects (manually and immediately) a Cisco 2600 series router or Cisco 3600 series router to the backup Cisco CallManager server.
mgcp call-agent	Defines the Cisco CallManager server as the highest priority.

ccm-manager sccp

To enable Cisco CallManager autoconfiguration of the Cisco IOS gateway, use the **ccm manager sccp** command in global configuration mode. To disable autoconfiguration, use the **no** form of this command.

ccm-manager sccp

no ccm-manager sccp

Syntax Description This command has no arguments or keywords.

Command Default Autoconfiguration is disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to trigger TFTP download of the eXtensible Markup Language (XML) configuration file. Issuing this command immediately triggers the download, and also enables the Skinny Client Control Protocol (SCCP) and SCCP Telephony Control Application (STCAPP), applications that enable Cisco CallManager control of gateway-connected telephony endpoints.

Examples The following example enables autoconfiguration of gateway-connected endpoints:

```
Router(config)# ccm-manager sccp
```

Related Commands

Command	Description
ccm-manager config	Specifies the TFTP server from which the Cisco IOS gateway downloads Cisco CallManager XML configuration files.
ccm-manager sccp local	Selects the local interface for SCCP application use for Cisco CallManager registration.
show ccm-manager config-download	Displays information about the status of the Cisco IOS gateway configuration download.

ccm-manager sccp local

To select the local interface that the Skinny Client Control Protocol (SCCP) application uses to register with Cisco CallManager, use the **ccm-manager sccp local** command in global configuration mode. To deselect the interface, use the **no** form of this command.

ccm-manager sccp local *interface-type interface-number*

no ccm-manager sccp local *interface-type interface-number*

Syntax Description

interface-type	Interface type that the SCCP application uses for Cisco CallManager registration.
interface-number	Interface number that the SCCP application uses for Cisco CallManager registration.

Command Default No local interface is selected.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines You must specify this interface before enabling the Cisco CallManager autoconfiguration process. The MAC address of this interface is used to identify gateway endpoints.

Examples The following example configures a FastEthernet interface for SCCP application use for Cisco CallManager registration:

```
Router(config)# ccm-manager sccp local fastethernet 0/0
```

Related Commands

Command	Description
show ccm-manager	Displays a list of Cisco CallManager servers and their current status and availability.

ccm-manager shut-backhaul-interfaces

To disable ISDN Layer 2 connectivity on a Cisco Call Manager Media Gateway Control Protocol (MGCP) PRI or BRI backhauled trunk when communication is lost between the Cisco Call Manager and the MGCP gateway, use the **ccm-manager shut-backhaul-interfaces** command in global configuration mode. To restore the default behavior, where ISDN Layer 2 is maintained between the MGCP gateway and the ISDN switch even when no connectivity exists between the MGCP gateway and any Cisco Call Manager, use the **no** form of this command.

ccm-manager shut-backhaul-interfaces

no ccm-manager shut-backhaul-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior is for the ISDN Layer 2 connection to be maintained (to make the Cisco Call Manager MGCP PRI or BRI backhaul continue to function) between the MGCP gateway and the ISDN switch even if no connectivity exists between the MGCP gateway and any Cisco Call Manager.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(8)	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(3f)	This command was integrated into Cisco IOS Release 12.4(3f).
12.4(5c)	This command was integrated into Cisco IOS Release 12.4(5c).
12.4(7c)	This command was integrated into Cisco IOS Release 12.4(7c).
12.4(4)T5	This command was integrated into Cisco IOS Release 12.4(4)T5.
12.4(6)T4	This command was integrated into Cisco IOS Release 12.4(6)T4.

Usage Guidelines

Use this command on Cisco IOS voice routers configured for Cisco Call Manager MGCP PRI or BRI backhaul.

Prior to the introduction of the **ccm-manager shut-backhaul-interfaces** command, a Cisco Call Manager MGCP PRI or BRI backhaul trunk would maintain ISDN Layer 2 connectivity between the MGCP gateway and the ISDN switch in a MULTIPLE_FRAMES_ESTABLISHED state even if Layer 3 Q.931 backhaul connectivity between the Cisco Call Manager and the MGCP gateway was unavailable. This causes problems because the ISDN switch interprets the PRI or BRI trunk as being active and continues to place calls to the MGCP gateway, even though all of the calls fail. After you enter the **ccm-manager shut-backhaul-interfaces** command, Layer 2 is disabled when connectivity between the Cisco Call Manager and the MGCP gateway is unavailable.

Examples

The following example disables ISDN Layer 2 connectivity on a Cisco Call Manager MGCP PRI or BRI backhauled trunk when communication is lost between Cisco Call Manager and the MGCP gateway:

```
ccm-manager shut-backhaul-interfaces
```

The following example restores the default behavior (functionality of the **ccm-manager shut-backhaul-interfaces** command is disabled) so that the ISDN Layer 2 connection is maintained between the MGCP gateway and the ISDN switch, even when no connectivity exists between the MGCP gateway and any Cisco Call Manager:

```
no ccm-manager mgcp
no ccm-manager shut-backhaul-interfaces
ccm-manager mgcp
```

Related Commands

Command	Description
ccm-manager mgcp	Enables the gateway to communicate with the Cisco Call Manager through the MGCP and to supply redundant control agent services.

ccm-manager shut-interfaces-tftp-fails

To configure the number of TFTP download failures allowed before the gateway shuts down ports, use the **ccm-manager shut-interfaces-tftp-fails** command in global configuration mode. To return to the default configuration, use the **no** form of this command.

ccm-manager shut-interfaces-tftp-fails *retries*

no ccm-manager shut-interfaces-tftp-fails

Syntax Description

retries	Number or TFTP retries. Range is from 2 to 10. The default is 2.

Command Default

Ports shut down after the second TFTP retry. However TFTP download attempts continue.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **ccm-manager shut-interfaces-tftp-fails** command to configure the number of TFTP download failures allowed before the gateway put the port in a shutdown state.

Examples

The following example shows a gateway being configured to put the port in a shutdown state after four TFTP download failures:

```
Router(config)# ccm-manager shut-interfaces-tftp-fails 4
```

Related Commands

Command	Description
show ccm-manager	Displays a list of Cisco Unified Communications Manager servers and their current status and availability.

ccm-manager switchback

To specify the time when control is to be returned to the primary Cisco CallManager server once it becomes available, use the **ccm-manager switchback** command in global configuration mode. To reset to the default, use the **no** form of this command.

ccm-manager switchback {**graceful** | **immediate** | **never** | **schedule-time** *hh*:*mm* | **uptime-delay** *minutes*}

no ccm-manager switchback

Syntax Description

graceful	Specifies that control is returned to the primary Cisco CallManager server after the last active call ends (when there is no voice call in active setup mode on the gateway). Default value.
immediate	Specifies an immediate switchback to the primary Cisco CallManager server when the TCP link to the primary Cisco CallManager server is established, regardless of current call conditions.
never	Specifies not to return control to the primary Cisco CallManager server, as long as the secondary is up and running. The gateway registers to primary if the secondary is down and when the primary is up and running.
schedule-time *hh*:*mm*	Specifies an hour and minute, based on a 24-hour clock, when control is returned to the primary Cisco CallManager server. If the specified time is earlier than the current time, the switchback occurs at the specified time on the following day.
uptime-delay *minutes*	Specifies the number of minutes the primary Cisco CallManager server must run after the TCP link to is reestablished and control is returned to that primary call agent. Valid values are from 1 to 1440 (1 minute to 24 hours).

Command Default

Graceful switchback

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was modified. This command was introduced with Cisco CallManager Version 3.0 on the Cisco VG200.
12.2(2)XA	The command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, 3600 series, and the Cisco VG200.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco IAD2420 series routers.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **never** keyword was added.

Usage Guidelines

This command allows you to configure switchback to the higher priority Cisco CallManager when it becomes available. Switchback allows call control to revert to the original (primary) Cisco CallManager once service has been restored.

Examples

In the following example, the primary Cisco CallManager is configured to be used as soon as it becomes available:

```
Router# configure terminal
Router(config)# ccm-manager switchback immediate
```

Related Commands

Command	Description
ccm-manager application	Configures the port number for the redundant link application.
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManagers.
ccm-manager switchover-to-backup	Redirects a Cisco 2600 series or Cisco 3600 series router to the backup Cisco CallManager.

ccm-manager switchover-to-backup

To manually redirect a gateway to the backup Cisco CallManager server, use the **ccm-manager switchover-to-backup** command in privileged EXEC mode.

ccm-manager switchover-to-backup

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XN	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series.

Usage Guidelines Switchover to the backup Cisco CallManager server occurs immediately. This command does not switch the gateway to the backup Cisco CallManager server if you have the **ccm-manager switchback** command option set to “immediate” and the primary Cisco CallManager server is still running.

Examples In the following example, the backup Cisco CallManager server is configured to be used as soon as it becomes available:

```
ccm-manager switchover-to-backup
```

Related Commands

Command	Description
ccm-manager application redundant-link	Configures the port number for the redundant link application (that is, for the secondary Cisco CallManager server).
ccm-manager redundant-host	Configures the IP address or the DNS name of up to two backup Cisco CallManager servers.
ccm-manager switchback	Specifies the time at which control is returned to the primary Cisco CallManager server once the server is available.

ccs connect (controller)

To configure a common channel signaling (CCS) connection on an interface configured to support CCS frame forwarding, use the **ccs connect** command in controller configuration mode. To disable the CCS connection on the interface, use the **no** form of this command.

ccs connect {**serial** | **atm**} *number* [*dlci* | **pvc** *vpi/vci* | **pvc** *name*] [*cidnumber*]

no ccs connect {**serial** | **atm**} *number* [*dlci* | **pvc** *vpi/vci* | **pvc** *name*] [*cidnumber*]

Syntax Description

serial	Makes a serial CCS connection for Frame Relay.
atm	Makes an Asynchronous Transfer Mode (ATM) CCS connection.
dlci	(Optional) Specifies the data link connection identifier (DLCI) number.
pvc *vpi/vci*	(Optional) Specifies the permanent virtual circuit (PVC) virtual path identifier or virtual channel identifier. Range is from 0 to 255; the slash is required.
pvc *name*	(Optional) Specifies the PVC string that names the PVC for recognition.
cidnumber	(Optional) If you have executed the **ccs encap frf11** command, the *cidnumber* argument allows you to specify any channel identification (CID) number from 5 to 255.

Command Default

No CCS connection is made.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	The *cidnumber* argument was added; the **dlci** keyword and **vcd** options were removed.
12.1(2)T	The CID syntax addition and removal of the **dlci** keyword and **vcd** options were integrated into Cisco IOS Release 12.1(2)T.
12.1(2)XH	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco 7500 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use this command to configure a CCS connection. If the CCS connection is over Frame Relay, specify a serial interface and the DLCI. If the CCS connection is over ATM, specify **atm**, the slot number, and the PVC.

If you have executed the **ccs encap frf11** command, the *cidnumber* option allows you to specify any CID from 5 to 255. If you do not issue the **ccs encap frf11** command, Cisco encapsulation is used, and any CID value other than 254 is ignored.

Note CDP and keepalives are disabled by default on a D-channel interface.

Examples

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 by using the default CID of 254, enter the following command:

```
ccs connect serial 1 100
```

or:

```
ccs connect serial 1 100 10
```

To configure a CCS frame-forwarding connection over an ATM PVC, enter the following command:

```
ccs connect atm0 pvc 100/10
```

or:

```
ccs connect atm0 pvc 10/100 21
```

or:

```
ccs connect atm0 pvc mypvc_10 21
```

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 using a CID of 110, enter the following command:

```
ccs connect serial 1 100 110
```

Related Commands

Command	Description
ccs encap frf11	Allows the specification of the standard Annex-C FRF.11 format.

ccs connect (interface)

To configure a common channel signaling (CCS) connection on an interface configured to support CCS frame forwarding, use the **ccs connect** command in interface configuration mode. To disable the CCS connection on the interface, use the **no** form of this command.

ccs connect {**serial** | **atm**} *number* [*dlci* | **pvc** *vpi/vci* | **pvc** *name*] [*cid-number*]

no ccs connect {**serial** | **atm**} *number* [*dlci* | **pvc** *vpi/vci* | **pvc** *name*] [*cid-number*]

Syntax Description

serial	Makes a serial CCS connection for Frame Relay.
atm	Makes an Asynchronous Transfer Mode (ATM) CCS connection.
dlci	(Optional) Data-link connection identifier (DLCI) number.
pvc *vpi/vci*	(Optional) Permanent virtual circuit (PVC) virtual path identifier or virtual channel identifier. Range is from 0 to 255; the slash is required.
pvc *name*	(Optional) PVC string that names the PVC for recognition.
cid-number	(Optional) If you have executed the **ccs encap frf11** command, the ***cid-number*** argument allows you to specify any channel identification (CID) number from 5 to 255.

Command Default No CCS connection is made.

Command Modes Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	The *cid-number* argument was added; the **dlci** keyword and **vcd** options were removed.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series router and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines Use this command to configure a CCS connection. If the CCS connection is over Frame Relay, specify a serial interface and the DLCI. If the CCS connection is over ATM, specify **atm**, the interface number (0), and the PVC. If you have executed the **ccs encap frf11** command, the *cid-number* option allows you to specify any CID from 5 to 255. If you do not issue the **ccs encap frf11** command, Cisco encapsulation is used, and any CID value other than 254 is ignored.

Note Cisco Discovery Protocol (CDP) and keepalives are disabled by default on a D-channel interface.

Examples

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 by using the default CID of 254, enter the following command:

```
ccs connect serial 1 100
```

or

```
ccs connect serial 1 100 10
```

To configure a CCS frame-forwarding connection over an ATM PVC, enter the following command:

```
ccs connect atm0 pvc 100/10
```

or

```
ccs connect atm0 pvc 10/100 21
```

or

```
ccs connect atm0 pvc mypvc_10 21
```

To configure a Frame Relay CCS frame-forwarding connection on DLCI 100 using a CID of 110, enter the following command:

```
ccs connect serial 1 100 110
```

Related Commands

Command	Description
ccs encap frf11	Allows the specification of the standard Annex-C FRF.11 format.

ccs encap frf11

To configure the common channel signaling (CCS) packet encapsulation format for FRF.11, use the **ccs encap frf11** command in interface configuration mode. To disable CCS encapsulation for FRF11, use the **no** form of this command.

ccs encap frf11

no ccs encap frf11

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the format is a Cisco packet format, using a channel ID (CID) of 254

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced for the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(2)XH	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco 7500 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command allows the specification of the standard Annex-C format. Use this command to define the packet format for the CCS packet; it places the FRF.11 Annex-C (Data Transfer Syntax) standard header on the CCS packets only.

Once the **ccs encap frf11** command is executed, you can use the **ccs connect** command to specify a CID other than 254.

Examples

The following example shows how to configure a serial interface for Frame Relay:

```
interface Serial1:15
 ccs encap frf11
 ccs connect Serial0 990 100
```

Related Commands

Command	Description
mode ccs frame-forwarding	Set to forward frames on the controller.

cdr-format

To select the format of the call detail records (CDRs) generated for file accounting, use the **cdr-format** command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

cdr-format {**compact** | **detailed**}

no cdr-format

Syntax Description

compact	Compact set of voice attributes is generated in CDRs.
detailed	Full set of voice attributes is generated in CDRs. Default value.

Command Default

Detailed (full version of CDRs is generated).

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command determines whether the CDRs generated by the file accounting process contain the complete set of voice attributes or a compact set of 17 voice attributes.

For a list of the complete set of voice attributes generated with the **detailed** keyword, see the "VSAs Supported by Cisco Voice Products" section in the *RADIUS VSA Voice Implementation Guide*.

The name and order of the attributes generated with the **compact** keyword are: CallLegType, ConnectionId, SetupTime, PeerAddress, PeerSubAddress, DisconnectCause, DisconnectText, ConnectTime, DisconnectTime, CallOrigin, ChargedUnits, InfoType, TransmitPackets, TransmitBytes, ReceivePackets, ReceiveBytes, feature_vsa.

Examples

The following example shows the CDR format set to compact:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 maximum buffer-size 60
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
acct-template	Selects a group of voice vendor-specific attributes to collect in accounting records.
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.

ces-clock

To configure the clock for the CES interface, use the **ces-clock** command in controller configuration mode. To disable the ces clock, use the **no** form of this command.

ces-clock {**adaptive | srts | synchronous**}

no ces-clock {**adaptive | srts | synchronous**}

Syntax Description

adaptive	Adjusts output clock on a received ATM Adaptation Layer 1 (AAL1) on first-in, first-out basis. Use in unstructured mode.
srts	Sets the clocking mode to synchronous residual time stamp.
synchronous	Configures the timing recovery to synchronous for structured mode.

Command Default

The default setting is synchronous

Command Modes

Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is used on Cisco 3600 series routers that have OC-3/STM-1 ATM CES network modules.

Examples

The following example configures the CES clock mode for synchronous residual time stamp:

```
ces-clock srts
```

Related Commands

Command	Description
controller	Configures the T1 or E1 controller.

cgma-agent

To enable the Cisco Gateway Management Agent (CGMA) on the Cisco IOS gateway, use the **cgma-agent** command in global configuration mode. To disable the CGMA, use the **no** form of this command.

cgma-agent [tcp-port *number***] | [time-period** *seconds***]**

no cgma-agent

Syntax Description

tcp-port *number*	(Optional) Specifies the TCP port number for the CGMA to use in communication with a third-party management system. Range is from 5000 to 65535. The default is 5000.
time-period *seconds*	(Optional) Specifies the maximum time period, in seconds for maintaining the link between the CGMA and the third-party management system during a period of inactivity. If twice the timeout value is met or exceeded with no message received from the client, the TCP connection is closed. Additionally, a 60-second timer is maintained in the CGMA, which closes the connection if no handshake query message is received from the third-party management system for 60 seconds. Range is from 45 to 300. The default is 45.

Command Default

Default *number* value is 5000.
Default *seconds* value is 45.

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5800 for this Cisco IOS release only.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release.

Usage Guidelines

Use this command to enable the CGMA on the Cisco IOS gateway. The CGMA communicates with the third-party management system to provide real-time information for gateway management, including the following:

- Handshake query, status query, and response messages between the CGMA and the third-party management system
- Call information such as start and end of call from call detail records (CDRs) sent using extensible markup language (XML) over TCP/IP
- Shows if T1 or E1 controllers and analog ports are up or down, and are also generated at the removal or addition of a “pri-group” or “ds0-group” under the T1 or E1 controller.

Examples

The following example shows that the CGMA is enabled on TCP port 5300 and that the CGMA times out after 300 seconds and closes its connection to the third-party management system because of inactivity in the link:

```
Router(config)# cgma-agent tcp-port 5300 time-period 300

Router# show running-config

Building configuration...

Current configuration : 1797 bytes
!
version 12.2
service config
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname gw1
!
.
.
.
resource-pool disable
!
ip subnet-zero
no ip domain-lookup
!
no ip dhcp-client network-discovery
isdn switch-type primary-ni
!
!
!
!
!
!
cgma-agent tcp-port 5300 time-period 300
fax interface-type modem
mta receive maximum-recipients 2
!
!
controller T1 0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
interface Ethernet0
 ip address 209.165.200.225 255.255.255.0
!
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice modem
 isdn T310 10000
 no cdp enable
!

voice-port 0:D
!
dial-peer voice 1213 voip
```

```
 destination-pattern 12135551000
 session target ipv4:209.165.200.229
!
dial-peer voice 1415 pots
 destination-pattern 14155551000
 direct-inward-dial
 port 0:D
!
dial-peer voice 12136 voip
 destination-pattern 12136661000
 session target ipv4:209.165.200.229
!
dial-peer voice 14156 pots
 incoming called-number .
 direct-inward-dial
!
gateway
!
end
```

channel-group

To configure serial WAN on a T1 or E1 interface, use the **channel-group** command in controller configuration mode. To clear a channel group, use the **no** form of this command.

Cisco 2600 Series

channel-group *channel-group-number* **timeslots** *range* [**speed** *kbps*] [**aim** *aim-slot-number*]

no channel-group *channel-group-number*

Cisco 2611 (Cisco Signaling Link Terminal [SLT])

channel-group *channel-number*

no channel-group *channel-number*

Cisco 2600XM Series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745

channel-group *channel-group-number* {**timeslots** *range* [**speed** {**56** | **64**}] | **unframed**} [**aim** *aim-slot-number*]

no channel-group [*channel-group-number* **timeslots** *range*]

Cisco AS5350 and Cisco AS5400 Series

channel-group *channel-group-number*

no channel-group *channel-group-number*

Cisco MC3810

channel-group *channel-number* **timeslots** *range* [**speed** *kbps*}]

no channel-group [*channel-number* **timeslots** *range*]

Syntax Description

channel-group-number	Channel-group number on the Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers. When a T1 data line is configured, channel-group numbers can be values from 0 to 23. When an E1 data line is configured, channel-group numbers can be values from 0 to 30. Valid values can be 0 or 1 on the Cisco AS5350 and Cisco AS5400.
timeslots *range*	Specifies one or more time slots separated by commas, or ranges of time slots belonging to the channel group separated by a dash. The first time slot is numbered 1. For a T1 controller, the time slots range from 1 to 24. For an E1 controller, the time slots range from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). See the "Examples" section for samples of different timeslot ranges.

speed {**56** | **64**}	(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64. The default line speed when configuring a T1 controller is 56 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810. The default line speed when configuring an E1 controller is 64 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810. The line speed controls real-time (VBR-RT) traffic shaping, and the maximum burst size (MBS) is 255 cells.
aim *aim-slot-number*	(Optional) Directs HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 digital signaling processor (DSP) card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.
channel-number	Number of the channel. Valid values can be 0 or 1 on the Cisco SLT (Cisco 2611).
unframed	Specifies the use of all 32 time slots for data. None of the 32 time slots are used for framing signals on the Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745. This is applicable to E1 only.

Command Default

The T1/E1 line is connected to the Motorola MPC-860x processor serial communication controller (SCC) or network module with two voice or WAN interface card (VIC or WIC) slots and 0/1/2 FastEthernet ports DSCC4 by default on Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.

There is no default behavior or values on the Cisco SLT (Cisco 2611).

The serial interface object encapsulation is set to HDLC on a network access server (NAS) (Cisco AS5350 and Cisco AS5400 series routers).

The default line speed is 56 kbps when a T1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

The default line speed is 64 kbps when an E1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.0	This command was integrated into Cisco IOS Release 12.0 on the Cisco MC3810.
12.0(7)XE	This command was implemented on the Catalyst 6000 family switches.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Release	Modification
12.1(1)T	This command was modified to accommodate two channel groups on a port on 1- and 2-port T1/E1 Multiflex voice or WAN interface cards on the Cisco 2600 and Cisco 3600 series routers.
12.1(3a)E3	The number of valid values for *kbps* was changed on the Cisco MC3810; see the "Usage Guidelines" section for valid values.
12.2(11)T	This command was modified for use on the Cisco AS5350 and Cisco AS5400.
12.2(11)T	The **aim** keyword was added for use on the Cisco 2600 series (including the Cisco 2691), Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(1)	The **unframed** keyword was added for use on the Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to direct High-Level Data Link Control (HDLC) traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card. A channel group is created using Advanced Integration Module (AIM) HDLC resources when a **channel-group** command with the **aim** keyword is parsed during system initialization or when the command is entered during configuration. You must specify the **aim** keyword under a T1/E1 controller port to direct HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.

Note Neither the Cisco AS5400 series NAS nor the Cisco MC3810 is supported with the integrated voice and data WAN on T1/E1 interfaces using the AIM-ATM-VOICE-30 module.

If previous **channel-group** commands are configured with the **aim** keyword, subsequent **channel-group** commands without the **aim** keyword are rejected. Similarly, if a regular **channel-group** command is followed by another **channel-group** command with the **aim** keyword implemented, the second command is rejected on the Cisco 2600 and Cisco 2600XM.

A channel group using AIM HDLC resources is deleted only when a **no channel-group** command is entered.

By default, the **channel-group** command on a NAS sets the serial interface object encapsulation to HDLC. You must override the default by entering the **encapsulation ss7** command for that serial interface object. Once you override the default, encapsulation cannot be changed again for that object. The SS7 encapsulation option is new to the **Integrated Signaling Link Terminal** feature and is available only for interface serial objects created by the **channel-group** command. The Integrated Signaling Link Terminal feature added SLT functionality on Cisco AS5350 and Cisco AS5400 platforms.

A digital SS7 link can be deleted by entering the **no channel-group** *channel-group-number* command on the associated T1/E1 controller. The link must first be stopped using the **no shutdown** command. It is not necessary to remove the channel ID association first.

Use the **channel-group** command in configurations where the router or access server must communicate with a T1 or E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. The time slot range must match the time slots assigned to the channel group. The service provider defines the time slots that comprise a channel group.

Note Channel groups, channel-associated signaling (CAS) voice groups, DS0 groups, and time-division multiplexing (TDM) groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, and TDM groups must be unique on the local Cisco MC3810 concentrator. For example, you cannot use the same group number for a channel group and for a TDM group. Furthermore, on the Cisco MC3810, only one channel group can be configured on a controller.

The channel group number can be 0 or 1 on the Cisco SLT (Cisco 2611).

The **channel-group** command also applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC on the Cisco MC3810.

Examples

The following example shows basic configuration directing HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card, starting in global configuration mode:

```
Router(config)# controller e1 1/0
Router(config-controller)# clock source internal
Router(config-controller)# channel-group 0 timeslots 1-31 aim 0
```

The following example explicitly sets the encapsulation type to PPP to override the HDLC default:

```
Router# configure terminal
Router(config)# controller t1 6/0
Router(config-controller)# channel-group 2 timeslots 3 aim 0
Router(config-controller)# exit
Router(config)# interface serial 6/0:2
Router(config-if)# encapsulation ppp
Router(config-if)# ip address 12.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example shows how to explicitly set the encapsulation type to SS7 to override the HDLC default using the Integrated Signaling Link Terminal feature. This example uses an 8PRI DFC card inserted into slot 7, and DS0-timeslot 3 on trunk 5 of that card is used as an SS7 link:

```
Router# configure terminal
Router(config)# controller t1 7/5
Router(config-controller)# channel-group 2 timeslots 3
Router(config-controller)# exit
Router(config)# interface serial 7/5:2
Router(config-if)# encapsulation ss7
Router(config-if)# channel-id 0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example defines three channel groups. Channel-group 0 consists of a single time slot, channel-group 8 consists of seven time slots and runs at a speed of 64 kbps per time slot, and channel-group 12 consists of two time slots.

```
Router(config-controller)# channel-group 0 timeslots 1
Router(config-controller)# channel-group 8 timeslots 5,7,12-15,20 speed 64
Router(config-controller)# channel-group 12 timeslots 2
```

The following example configures a channel group on controller T1 0 on a Cisco MC3810:

```
Router(config)# controller T1 0
Router(config-controller)# channel-group 10 timeslots 10-64
```

The following example configures a channel group on controller E1 1 and specifies that all time slots are used for data:

```
controller e1 1
channel-group 1 unframed
```

Note SS7 digital F-link support for the 8PRI line card requires use of a third onboard TDM stream to route trunk DS0 messages to the onboard Media Gateway Controllers (MGCs).

Related Commands

Command	Description
framing	Specifies the frame type for the T1 or E1 data line.
invert data	Enables channel inversion.
linecode	Specifies the line code type for the T1 or E1 line.
voice-card	Configures a card with voice processing resources and enters voice card configuration mode.

channel-id

To assign a session channel ID to an SS7 serial link or assign an SS7 link to an SS7 session set on a Cisco AS5350 or Cisco AS5400, use the **channel-id** command in interface configuration mode. To disable a session channel ID link, use the **no** form of this command.

channel-id *channel-id* [**session-set** *session-set-id*]

no channel-id

Syntax Description

channel-id	Selects a unique session channel ID. This session channel ID is needed when the link with a Reliable User Datagram Protocol (RUDP) session to the media gateway controller (MGC) is associated.
session-set *session-set-id*	(Optional) Creates an SS7-link-to-SS7-session-set association on the Cisco AS5350- and Cisco AS5400-based Cisco Signaling Link Terminals (SLTs). The *session-set-id* argument represents the SS7 session ID. Valid values are 0 or 1. Default is 0.

Command Default No default behavior or values

Command Modes Interface configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	The **session-set** *session-set-id* keyword and argument were added.

Usage Guidelines The **channel-id** command is visible only if the object's encapsulation type is changed to SS7.

Before an SS7 serial link can be enabled using the **no shutdown** command, you must enter the **channel-id** command in interface configuration mode to assign a session channel ID to the SS7 serial link. This ID is unique to the Cisco AS5350 and Cisco AS5400, and the command is visible only for provisioned objects whose encapsulation type is the new SS7 value.

The channel identifier is reserved when you explicitly assign an ID using the **channel-id** command for the associated serial interface object. This fails if the selected channel identifier is currently assigned to another link or if all channel identifiers are already assigned.

A channel identifier is released when the **no channel-id** command is entered. The link must first be shut down to do this. If the **no channel-id** command is used with the Mulitple OPC Support for the Cisco Signaling Link Terminal feature, the associated SS7 link has no channel ID. In this state the link is not fully configured and is incapable of supporting signaling traffic.

If the **session-set** keyword is omitted, the command is applied to SS7 session set 0, which is the default. Reissuing the **session-set** keyword with a different SS7 session ID is sufficient to remove the associated SS7 link from its existing SS7 session set and add it to the new one.

Examples

The following example shows a unique session channel ID zero being assigned to the Cisco AS5350 or Cisco AS5400:

```
Router(config-if)# channel-id 0
```

The following example assigns an SS7 link to an SS7 session set on a Cisco AS5350 or Cisco AS5400:

```
Router(config-if)# channel-id 0 session-set 1
```

Related Commands

Command	Description
channel-group	Assigns a channel group and selects the DS0 timeslot(s) desired for SS7 links.
encapsulation ss7	Sets the encapsulation type to SS7.
no shutdown	Changes the administrative state of a port from out-of-service to in-service.
session-set	Creates a Signaling System 7 (SS7)-link-to-SS7-session-set association or to associate an SS7 link with an SS7 session set on the Cisco 2600-based Signaling Link Terminal (SLT).
ss7 mtp2 variant bellcore	Configures the device for Telcordia (formerly Bellcore) standards. This command is hidden in the running configuration with this feature.

clear backhaul-session-manager group stats

To reset the statistics or traffic counters for a specified session group, use the **clear backhaul-session-manager group stats** command in privileged EXEC mode.

clear backhaul-session-manager group stats {**all** | **name** *group-name*}

Syntax Description

all	All available session groups.
name *group-name*	A specified session group.

Command Default The statistical information accumulates

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines A session is the connection between a client and a server, and a session group is a collection of sessions in a group to implement switchover in case of a session failure. This command clears all statistics that pertain to the backhaul session manager group.

Examples The following example clears all statistics for all available session groups:

```
Router(config)# clear backhaul-session-manager group stats all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified group or all session groups.

clear call application interface

To clear application interface statistics and event logs, use the **clear call application interface** command in privileged EXEC mode.

clear call application interface [[{**aaa** | **asr** | **flash** | **http** | **ram** | **rtsp** | **smtp** | **tftp** | **tts**} [**server** *server*]] [**event-log** | **stats**]]

Syntax Description

event-log	(Optional) Clears event logs.
stats	(Optional) Clears statistic counters.
aaa	Authentication, authorization, and accounting (AAA) interface type.
asr	Automatic speech recognition (ASR) interface type.
flash	Flash memory of the Cisco gateway.
http	Hypertext Transfer Protocol (HTTP) interface type.
ram	Memory of the Cisco gateway.
rtsp	Real-time Streaming Protocol (RTSP) interface type.
smtp	Simple Mail Transfer Protocol (SMTP) interface type.
tftp	Trivial File Transfer Protocol (TFTP) interface type.
tts	Text-to-speech (TTS) interface type.
server *server*	(Optional) Clears statistics or event logs for the specified server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command resets statistic counters to zero and clears event logs for application interfaces. If you do not use any keywords or arguments, this command clears statistics and event logs for all application interfaces.

Examples

The following example clears statistics and event logs for application interfaces:

```
Router# clear call application interface
```

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface stats	Enables statistics collection for application interfaces.

Command	Description
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application interface	Displays event logs and statistics for application interfaces.

clear call application stats

To clear application-level statistics in history and subtract the statistics from the gateway-level statistics, use the **clear call application stats** command in privileged EXEC mode.

clear call application [**app-tag** *application-name*] **stats**

Syntax Description

app-tag *application-name*	(Optional) Clears statistics for the specified voice application.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command resets application-level counters in history to zero and subtracts the counters from the gateway-level history. If you do not specify an application name, this command clears statistics for all applications at the application level and gateway level.

Note Statistic counters are automatically cleared for an application if the application is deleted with the **no call application voice** command or the script is reloaded with the **call application voice load** command.

Examples

The following example clears statistics for the application named sample_app:

```
Router# clear call application stats sample_app
```

Related Commands

Command	Description
call application stats	Enables statistics collection for voice applications.
clear call application interface	Clears application interface statistics and event logs.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.

clear call fallback cache

To clear the cache of the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses or a specific IP address, use the **clear call fallback cache** command in EXEC mode.

clear call fallback cache [*ip-address*]

Syntax Description

ip-address	(Optional) Specifies the target IP address. If no IP address is specified, all IP addresses are cleared.

Command Default If no IP address is specified, all IP addresses are cleared.

Command Modes EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series routers and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines If no IP address is specified, this command clears the cache of all ICPIF estimates for all IP addresses.

Examples The following example clears the cache of the ICPIF estimate for IP address 10.0.0.0:

```
Router# clear call fallback cache 10.0.0.0
```

Related Commands

Command	Description
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the call fallback cache.

clear call fallback stats

To clear the call fallback statistics, use the **clear call fallback stats** command in EXEC mode.

clear call fallback stats

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(4)T	The PSTN Fallback feature and enhancements were implemented on Cisco 7200 series and integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example clears the call fallback statistics:

```
Router# clear call fallback stats
```

Related Commands

Command	Description
show call fallback stats	Displays the call fallback statistics.

clear callmon

To clear call monitor logs, use the **clear callmon** command in privileged EXEC mode.

clear callmon {**dead-memory** | **trace**}

Syntax Description

dead-memory	Clears unreleased Communication Media Module (CMM) line card memory.
trace	Clears CMM trace buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to clear unreleased CMM memory:

```
Router# clear callmon dead-memory
```

The following example shows how to clear CMM trace buffers:

```
Router# clear callmon trace
```

Related Commands

Command	Description
clear tgrep neighbor	Clears TGREP counters and sessions.

clear call threshold

To clear enabled call threshold statistics, use the **clear call threshold command in privileged** EXEC mode.

clear call threshold {**stats | total-calls** [*value*] | **interface** *int-name* **int-calls** [*value*]}

Syntax Description

stats	Resets all call threshold statistics.
total-calls	Resets the counter when the call volume reaches the specified number.
value	Represents call volume. Range is from 0 to 10000 calls. The default is 0.
interface *int-name*	Specifies the interface through which calls arrive. Types of interfaces and their numbers depends upon the configured interfaces.
int-calls	Number of calls transmitted through the interface.
value	Clears calls when they reach a specified volume through the interface. Range is from 0 to 10000 calls. The default is 0.

Command Default

The default setting of 0 for **total-calls** and **int-calls** resets all threshold statistics immediately. **stats** is the default keyword.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400, is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following example resets all call threshold statistics:

```
clear call threshold stats
```

The following example also resets the counter for all call volume in the gateway:

```
clear call threshold total-calls
```

The following example resets the counter when the call volume on Ethernet interface 0/1 reaches 5000 calls:

```
clear call threshold interface ethernet 0/1 int-calls 5000
```

Related Commands

Command	Description
call threshold	Enables the global resources of a gateway.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
show call treatment	Displays the call treatment configuration and statistics for handling the calls on the basis of resource availability.

clear call treatment stats

To clear call treatment statistics, use the **clear call treatment stats** command in privileged EXEC mode.

clear call treatment stats

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Examples The following example clears the call treatment statistics:

```
clear call treatment stats
```

Related Commands

Command	Description
call treatment on	Enables call treatment to process calls when local resources are unavailable.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause-code for ISDN calls when local resources are unavailable.
show call treatment	Displays the call treatment configuration and statistics for handling calls on the basis of resource availability.

clear call voice

To clear one or more voice calls detected as inactive because there is no RTP or RTCP activity, use the **clear call voice** command in EXEC or privileged EXEC mode.

clear call voice causecode *identifier*{**id** *identifier* | **media-inactive** | **calling-number** *number* | **called-number** *number*}

Syntax Description

causecode	Specifies a Q.850 disconnect cause code.
identifier	Numeric cause code identifier; a number 1 through 127.
id	Clears one specific call with the ID specified.
identifier	Call identifier as shown in brief format.
media-inactive	Clears calls wherever a status of media inactive is detected and notified.
calling-number	Clears a call with a specific calling number pattern.
called-number	Clears a call with a specific called number pattern.
number	Specific call number pattern of a called number or calling number.

Command Default

This command is disabled, and no calls are cleared.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3(4)T	The **voice** keyword was added.
12.4(4)T	The **calling-number** and **called-number** keywords were added.

Usage Guidelines

This command can be used to clear all voice calls detected as media inactive or it can be used to clear individual voice calls. There is no **no** form of this command.

Examples

The following example clears inactive voice calls with the cause code ID of 112B:

```
Router# clear call voice causecode 1 id 112B
```

Related Commands

Command	Description
show call active voice	Displays active voice calls, based on specified parameters.

clear call-router routes

To remove the dynamic routes cached in the border element (BE), enter the **clear call-router routes** command in privileged EXEC mode.

clear call-router routes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example shows how to remove dynamic routes cached in the BE:

```
Router# clear call-router routes
```

Related Commands

Command	Description
call-router	Enables the Annex G BE configuration commands.
show call history	Displays the fax history table for a fax transmission.

clear controller call-counters

To clear the system DS0 high water marks (HWM) and all individual controller statistics, use the **clear controller call-counters** command in privileged EXEC mode.

clear controller call-counters {**system-hwm** | **all**}

Syntax Description

system-hwm	Clears the system HWMs only.
all	Clears *all* controller call counters including the individual controller time slots in use and the number of calls on those time slots since the last reset was done. The HWMs are set to 0.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	This command was implemented on the voice/WAN interface cards (VWICs) for Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5800.

Usage Guidelines The **clear controller call-counters all** command clears the system DS0 HWMs and all individual controller statistics, including Total Calls and Total Duration. The **clear controller call-counters system-hwm** command clears the system DS0 HWMs and leaves all other call-counter statistics untouched.

Refer to the comments below for the meaning of call counters displayed before and after executing **clear controller call-counters** and **clear controller t1 call-counters** related commands.

- The numbers displayed under TotalCalls for each time slot represent *total* calls that were connected successfully. If a call comes into time slot 10, then the **show controllers t1 call-counters** command displays 1 under the TotalCalls column for time slot 10. A value of 20 displayed under TotalCalls for time slot 10 indicates a total of 20 calls connected on time slot 10 since the last time call counters were cleared.
- The DS0s Active field indicates the number of active calls on the specified controller. This number indicates the current number of calls on the controller at any given time.
- The DS0s Active High Water Mark field indicates the peak number of calls on the controller since the last time HWMs or calls were cleared. If the number of active calls “DS0s Active” is less than DS0s HWM, then HWM remains untouched. If new calls come in and the active DS0s are more than the HWM, then the HWM is incremented to reflect the new peak number of calls on that controller.

This value is reset to the current and active DS0s when call counters are cleared. For example, initially the HWM is 0. When a new call comes in, the HWM is 1. When the next call comes in, the HWM is 2.

If 20 calls come in, the HWM is 20 and the active DS0s are 20. If 5 calls get disconnected, the DS0 active is 15, but the HWM is 20. When a **clear controller** command is input for the specified controller, the HWM is reset to 15, which is the current and active DS0s also. If 10 calls get disconnected, the Active DS0s is set to 5 and the HWM remains at 15 until another **clear controller command** is input. If Active DS0s exceed 15, then the HWM is updated.

- The System DS0s High Water Mark field reflects the HWM at a system level including all DS0s controllers.

Examples

The following sample output shows what happens after the HWMs are cleared:

```
Router# clear controller call-counters system-hwm
!
Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           1       00:08:51
     23       pri           1       00:09:21
T1 1/3/0:8:
  DS0's Active: 1
  DS0's Active High Water Mark: 1
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
```

```
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            0       00:01:39
     23       pri            0       00:00:00

System's DS0's Active High Water Mark: 3
```

In the example above, the system HWM is reset to the total number of active calls in the system, which is 3. The number was 4. When a call goes down, HWM values are untouched. Only the DS0 Active value changes. Above, there is only one call on 1/3/0:3. Observe the HWM for individual controllers. Total number of active calls is 1.

The following is sample output when the **clear controller call-counters system-hwm** command is used:

```
Router# clear controller call-counters system-hwm
!
Router# show controllers t1 call-counters
T1 1/3/0:3:
  DS0's Active: 1
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:12:16
     23       pri            1       00:10:20
T1 1/3/0:8:
  DS0's Active: 0
  DS0's Active High Water Mark: 1
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
```

```
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           0       00:02:50
     23       pri           0       00:00:00

System's DS0's Active High Water Mark: 1
```

In the previous example, only the system HWM is reset to active. For controllers 1/3/0:3 and 1/3/0:8, the HWMs are untouched.

The following is sample output when the **all** keyword is used, clearing at the system level:

```
Router# clear controller call-counters all
!
Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           0       00:00:00
     23       pri           0       00:00:00
T1 1/3/0:8:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
```

```
      7       pri             0       00:00:00
      8       pri             0       00:00:00
      9       pri             0       00:00:00
     10       pri             0       00:00:00
     11       pri             0       00:00:00
     12       pri             0       00:00:00
     13       pri             0       00:00:00
     14       pri             0       00:00:00
     15       pri             0       00:00:00
     16       pri             0       00:00:00
     17       pri             0       00:00:00
     18       pri             0       00:00:00
     19       pri             0       00:00:00
     20       pri             0       00:00:00
     21       pri             0       00:00:00
     22       pri             0       00:00:00
     23       pri             0       00:00:00
System's DS0's Active High Water Mark: 0
```

In the previous example, clearing at the system level using the **clear controller call-counters** command clears all DS0 controllers in the system and also clears the system HWMs.

The following is sample output showing four active calls:

Related Commands

Command	Description
clear controller t1 call-counters	Clears call statistics on a specific T1 controller.
controller	Enters controller configuration mode.
show controllers t1 call-counters	Displays the total number of calls and call durations on a T1 controller.

clear controller t1

To clear the system DS0 high water marks (HWM) and all individual controller statistics, use the **clear controller t1** command in privileged EXEC mode.

clear controller t1 [*slot*] **call-counters** *timeslots* | **firmware-status**

slot	(Optional) Clears an individual T1 controller.
call-counters *timeslots*	Clears the call counters in the specified T1 time slots.
firmware-status	Clears the Neat crash history.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	This command was implemented on the voice and WAN interface cards (VWICs) for Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5800.

Usage Guidelines Refer to the comments below for the meaning of call counters displayed before and after executing **clear controller t1 call-counters** related commands.

- The numbers displayed under TotalCalls for each time slot represent *total* calls that were connected successfully. If a call comes into time slot 10, then the **show controllers t1 call-counters** command displays 1 under the TotalCalls column for time slot 10. A value of 20 displayed under TotalCalls for time slot 10 indicates a total of 20 calls connected on time slot 10 since *the last time call counters were cleared*.

  If a timeslot or timeslot range is specified, only the counters for those channels are cleared. The TotalCalls field shows the time slots that have calls connected since the last clear was done and does not show the number of active calls in the controller. The TotalDuration field shows the same information as the TotalCalls field.

- The DS0s Active field indicates the number of active calls on the specified controller. This number indicates the current number of calls on the controller at any given time.

- The DS0s Active High Water Mark field indicates the peak number of calls on the controller since the last **clear controller t1 1/0/0 call-counters** command was entered. If the number of active calls "DS0s Active" is less than DS0s HWM, then HWM remains untouched. If new calls come in and the active DS0s are more than the HWM, then the HWM is incremented to reflect the new peak number of calls on that controller.

  This value is reset to the *current* and active DS0s when the **clear controller t1 1/3/0 call-counters** command is entered. For example, initially the HWM is 0. When a new call comes in, the HWM is 1. When the next call comes in, the HWM is 2.

If 20 calls come in, the HWM is 20 and the active DS0s are 20. If 5 calls get disconnected, the DS0 active is 15, but the HWM is 20. When a **clear controller** command is input for the specified controller, the HWM is reset to 15, which is the current and active DS0s also. If 10 calls get disconnected, the Active DS0s is set to 5 and the HWM remains at 15 until another **clear controller command** is input. If Active DS0s exceed 15, then the HWM is updated.

- The System DS0s High Water Mark field reflects the HWM at a system level including all DS0s controllers.

Examples

The following is sample output that shows two controllers numbered 1/3/0:3 and 1/3/0:8. Note the differences in the output shown by the **show controllers t1 call-counters** command and how the **clear controller t1 call-counters** command affects the output:

```
Router#  show controllers t1 call-counters
T1 1/3/0:3:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           0       00:00:00
     23       pri           0       00:00:00
T1 1/3/0:8:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
```

```
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            0       00:00:00
     23       pri            0       00:00:00

System's DS0's Active High Water Mark: 0
```

Note In the previous example, all the fields are zero indicating that no calls have come in since system startup or since the last clear was made by the **clear controller** command.

The following is sample output that shows that four calls have been initiated on the 1/5/12, 1/5/13, 1/5/14, and 1/5/15 controllers:

```
Router# show users

    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
  tty 1/5/12   Router Async interface      00:01:05   PPP: 55.61.1.1
  tty 1/5/13   Router Async interface      00:00:48   PPP: 55.62.1.1
  tty 1/5/14   Router Async interface      00:00:33   PPP: 55.54.1.1
  tty 1/5/15   Router Async interface      00:00:19   PPP: 55.52.1.1

  Interface  User      Mode                     Idle Peer Address

Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:01:58
     23       pri            1       00:02:27
T1 1/3/0:8:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
```

```
     2       pri            0       00:00:00
     3       pri            0       00:00:00
     4       pri            0       00:00:00
     5       pri            0       00:00:00
     6       pri            0       00:00:00
     7       pri            0       00:00:00
     8       pri            0       00:00:00
     9       pri            0       00:00:00
    10       pri            0       00:00:00
    11       pri            0       00:00:00
    12       pri            0       00:00:00
    13       pri            0       00:00:00
    14       pri            0       00:00:00
    15       pri            0       00:00:00
    16       pri            0       00:00:00
    17       pri            0       00:00:00
    18       pri            0       00:00:00
    19       pri            0       00:00:00
    20       pri            0       00:00:00
    21       pri            0       00:00:00
    22       pri            1       00:02:14
    23       pri            1       00:02:46

System's DS0's Active High Water Mark: 4
```

In the example above, if a **clear controller** command is entered for a controller that has active calls, which have been connected during the last 30 minutes, the TotalCalls and TotalDuration fields are reset to zero.

The following is sample output that shows controller 1/3/0:3, with time slots 22 and 23 connected and active. When the **clear controller t1 1/3/0:3 call-counters** command is entered, the corresponding fields are set to zero.

```
Router# clear controller t1 1/3/0:3 call-counters
!
Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:29:14
```

```
     23       pri           1       00:29:47

Router# clear controller t1 1/3/0:3 call-counters

Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           0       00:00:10   <<<<<<
     23       pri           0       00:00:10   <<<<<<
```

The following is sample output when a call is cleared on 1/5/12:

```
Router# clear line 1/5/12

[confirm]
 [OK]
!
Router# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
  tty 1/5/13   Router Async interface      00:03:04   PPP: 55.62.1.1
  tty 1/5/14   Router Async interface      00:02:49   PPP: 55.54.1.1
  tty 1/5/15   Router Async interface      00:02:35   PPP: 55.52.1.1

  Interface  User      Mode                     Idle Peer Address

Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
```

```
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:03:44
     23       pri            1       00:04:14
T1 1/3/0:8:
  DS0's Active: 1
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:04:00
     23       pri            1       00:03:34

System's DS0's Active High Water Mark: 4
```

After a call gets disconnected, only the DS0 Active field changes to reflect the current active call on the controller. In the above example, 1/3/0:8 DS0 Active is changed to 1.

The following is sample output that shows call counters are cleared for an individual controller on 1/3/0:8:

```
Router# clear controller t1 1/3/0:8 call-counters
!
Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
```

```
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            1       00:07:46
     23       pri            1       00:08:15
T1 1/3/0:8:
  DS0's Active: 1
  DS0's Active High Water Mark: 1
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri            0       00:00:00
      2       pri            0       00:00:00
      3       pri            0       00:00:00
      4       pri            0       00:00:00
      5       pri            0       00:00:00
      6       pri            0       00:00:00
      7       pri            0       00:00:00
      8       pri            0       00:00:00
      9       pri            0       00:00:00
     10       pri            0       00:00:00
     11       pri            0       00:00:00
     12       pri            0       00:00:00
     13       pri            0       00:00:00
     14       pri            0       00:00:00
     15       pri            0       00:00:00
     16       pri            0       00:00:00
     17       pri            0       00:00:00
     18       pri            0       00:00:00
     19       pri            0       00:00:00
     20       pri            0       00:00:00
     21       pri            0       00:00:00
     22       pri            0       00:00:35
     23       pri            0       00:00:00

System's DS0's Active High Water Mark: 4
```

In the previous example, after clearing call counters for controller 1/3/0:8, TotalCalls and TotalDuration reset. In addition the DS0 HWM is also *cleared* to the number of active DS0s. Whenever the DS0 HWM is cleared, it does not reset to zero, but rather it is set to Active DS0s. For 1/3/0:8, the HWM is 1 after clearing because DS0 Active is 1 (1 active call). TotalDuration is 35 seconds for time slot 22, and TotalCall is 0 because they got reset when the **clear controller call-counters** command was entered. Total calls on this time slot is incremented when a new call comes in on this time slot.

The following is sample output when controller 1/5/15 is cleared:

```
Router# clear line 1/5/15
[confirm]
 [OK]
Router# show controllers t1 call-counters

T1 1/3/0:3:
```

```
  DS0's Active: 0
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           1       00:12:40
     23       pri           1       00:10:20
T1 1/3/0:8:
  DS0's Active: 0
  DS0's Active High Water Mark: 1
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           0       00:02:50
     23       pri           0       00:00:00

System's DS0's Active High Water Mark: 1
```

The following is sample output showing four active calls:

```
Router# show users

Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
  tty 1/5/16   Router Async interface      00:01:01   PPP: 55.1.1.1
  tty 1/5/17   Router Async interface      00:00:47   PPP: 55.2.1.1
```

```
  tty 1/5/18   Router Async interface      00:00:28   PPP: 55.3.1.1
  tty 1/5/19   Router Async interface      00:00:14   PPP: 55.4.1.1

  Interface  User      Mode                     Idle Peer Address

Router# show controllers t1 call-counters

T1 1/3/0:3:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           1       00:00:57
     23       pri           1       00:01:30
T1 1/3/0:8:
  DS0's Active: 2
  DS0's Active High Water Mark: 2
  TimeSlot   Type   TotalCalls   TotalDuration
      1       pri           0       00:00:00
      2       pri           0       00:00:00
      3       pri           0       00:00:00
      4       pri           0       00:00:00
      5       pri           0       00:00:00
      6       pri           0       00:00:00
      7       pri           0       00:00:00
      8       pri           0       00:00:00
      9       pri           0       00:00:00
     10       pri           0       00:00:00
     11       pri           0       00:00:00
     12       pri           0       00:00:00
     13       pri           0       00:00:00
     14       pri           0       00:00:00
     15       pri           0       00:00:00
     16       pri           0       00:00:00
     17       pri           0       00:00:00
     18       pri           0       00:00:00
     19       pri           0       00:00:00
     20       pri           0       00:00:00
     21       pri           0       00:00:00
     22       pri           1       00:01:12
     23       pri           1       00:01:45

System's DS0's Active High Water Mark: 4
```

Related Commands

Command	Description
clear controller call-counters	Clears all call statistics or system HWMs on a router.
controller	Enters controller configuration mode.
show controllers t1 call-counters	Displays the total number of calls and call durations on a T1 controller.

clear csm-statistics modem

To clear the call switching module (CSM) statistics for a modem or group of modems, use the **clear csm-statistics modem** command in privileged EXEC mode.

clear csm-statistics modem [*slot/port* | *modem-group-number*]

Syntax Description

slot/port	(Optional) Identifies the location (and thereby the identity) of a specific modem.
modem-group-number	(Optional) Designates a defined modem group.

Command Default

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced.

Usage Guidelines

Use the **clear csm-statistics modem** command to clear CSM statistics for a particular modem or group of modems. If the *slot/port* argument is specified, the CSM call statistics for calls using the identified modem is cleared. If a modem group number is specified, then the CSM call statistics for calls using the modems associated with that group are cleared. If no argument is specified, all CSM call statistics for all modems are cleared.

Examples

The following example clears CSM call statistics for calls coming in on modems associated with modem group 2:

```
Router# clear csm-statistics modem 2
```

Related Commands

Command	Description
clear csm-statistics voice	Clears the CSM statistics for a particular or for all DSP channels.

clear csm-statistics voice

To clear the call switching module (CSM) statistics for a particular or for all digital signal processor (DSP) channels, use the **clear csm-statistics voice** command in privileged EXEC mode.

clear csm-statistics voice [*slot/dspm/dsp/dsp-channel*]

Syntax Description

slot/dspm/dsp/dsp-channel	(Optional) Identifies the location of a particular DSP channel.

Command Default

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced.

Usage Guidelines

Use the **clear csm-statistics voice** command to clear CSM statistics for a particular DSP channel. If the *slot/dspm/dsp/dsp-channel* argument is specified, the CSM call statistics for calls using the identified DSP channel are cleared. If no argument is specified, all CSM call statistics for all DSP channels are cleared.

Examples

The following example clears CSM call statistics for calls coming in on all DSP channels:

```
Router# clear csm-statistics voice
```

Related Commands

Command	Description
clear csm-statistics modem	Clears the CSM statistics for a modem or group of modems.

clear h323 gatekeeper call

To force the disconnection of a specific call or of all calls active on a particular gatekeeper, use the **clear h323 gatekeeper call** command in privileged EXEC mode.

clear h323 gatekeeper call {**all** | **local-callID** *local-callID*}

Syntax Description

all	Forces all active calls currently associated with this gatekeeper to be disconnected.
local-callID	Forces a single active call associated with this gatekeeper to be disconnected.
local-callID	Specifies the local call identification number (CallID) that identifies the call to be disconnected.

Command Default No default behaviors or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and on the Cisco MC3810.
12.1(5)XM2	The command was introduced for the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco AS5300. Support for the Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines If you want to force a particular call to be disconnected (as opposed to all active calls on the gatekeeper), use the CallID number to identify that specific call. You can find the local CallID number for a specific call by using the **show gatekeeper calls** command; the ID number is displayed in the LocalCallID column.

Examples The following example shows that an active call on the gatekeeper is being forced to disconnect. The local ID number of the active call is 12-3339.

```
Router# clear h323 gatekeeper call local-callID 12-3339
```

The following example shows that all active calls on the gatekeeper are being forced to disconnect:

```
Router# clear h323 gatekeeper call all
```

The following sample output from the **show gatekeeper calls** command displays information about a specific active call having a call ID of 12-3339:

```
Router# show gatekeeper calls
```

```
Total number of active calls =1
                    Gatekeeper Call Info
                    ====================
LocalCallID                     Age (secs)      BW
12-3339                         94              768 (Kbps)
 Endpt(s): Alias    E.164Addr     CallSignalAddr   Port   RASSignalAddr    Port
   src EP: epA                    10.0.0.11        1720   10.0.0.11        1700
   dst EP: epB2zoneB.com
   src PX: pxA                    10.0.0.1         1720   10.0.0.11        24999
   dst PX: pxB                    172.21.139.90    1720   172.21.139.90    24999
```

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.

clear h323 gatekeeper endpoint

To unregister endpoints, use the **clear h323 gatekeeper endpoint** command in privileged EXEC mode.

clear h323 gatekeeper endpoint {alias e164 ***digits*** **| alias h323id** ***name*** **| all | id** ***number*** **| ipaddr** ***address*** **[***port***]}**

Syntax Description

alias e164 *digits*	E.164 alphanumeric address that is specified in the local alias table.
alias h323id *name*	H.323 ID name that is specified in the local alias table and is an alternate way to reach an endpoint.
all	All endpoints.
id *number*	ID of the endpoint.
ipaddr *address* [*port*]	Call signaling address and port (optional) of the endpoint. If a value for the *port* argument is not specified, the default is 1720.

Command Default

Default for the *port* argument is 1720.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3660 and Cisco MC3810.

Usage Guidelines

Using this command forces the gatekeeper to send an unregistration request (URQ) message to the specified endpoint or all endpoints and removes the endpoint from the gatekeeper registration database.

For gatekeeper cluster configurations, this command must be entered on the gatekeeper where the endpoint is registered. Use the **show gatekeeper endpoints** command to locate the endpoint in a gatekeeper cluster.

Note The endpoint that was unregistered using this command can come back if it sends the registration request (RRQ) back to the gatekeeper after the unregistration.

Examples

The following example shows how to unregister all endpoints:

```
GK# clear h323 gatekeeper endpoint all
GK# show gatekeeper endpoints

                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
Total number of active registrations = 0
```

Related Commands

Command	Description
show gatekeeper endpoints	Locates the endpoint in a gatekeeper cluster.

clear h323 gatekeeper stats

To clear statistics about gatekeeper performance, use the **clear h323 gatekeeper stats** command in privileged EXEC mode.

clear h323 gatekeeper stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

The **clear h323 gatekeeper stats** command resets the gatekeeper performance counters to zero and records the time at which the last clear was performed.

Examples

The following is sample output from the **show gatekeeper performance stats** command that shows the counters have been reset to zero after entering the **clear h323 gatekeeper stats** command.

```
clear h323 gatekeeper stats
show gatekeeper performance stats

RAS inbound message counters:
Originating ARQ: 0 Terminating ARQ: 0 LRQ: 0
RAS outbound message counters:
ACF: 2  ARJ: 0 LCF: 2  LRJ: 0
ARJ due to overload: 0
LRJ due to overload: 0
Load balancing events: 0
Real endpoints: 2
```

Related Commands

Command	Description
show gatekeeper performance statistics	Displays information about the number of calls accepted and rejected by the gatekeeper.

clear h323 gateway

To clear the H.323 gateway counters, use the **clear h323 gateway command in privileged EXEC mode.**

clear h323 gateway [**cause-code stats | h225 | ras**]

Syntax Description

cause-code stats	(Optional) Clears only the disconnect cause-code statistics counters.
h225	(Optional) Clears only the H.225 counters.
ras	(Optional) Clears only the Registration, Admission, and Status (RAS) counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced on all Cisco H.323 platforms except for the Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

To clear all H.323 counters, use the **clear h323 gateway** command without any of the optional keywords. After you have used the **clear h323 gateway** command, the respective counters are set to zero.

Examples

In the following example from a Cisco 3640 router, the **clear h323 gateway** command is used without keywords to clear all H.323 counters:

```
Router# clear h323 gateway

All H.323 stats cleared at 01:54:38
```

In the following example from a Cisco 3640 router, the **clear h323 gateway** command is used with the **cause-code stats** keyword to clear the disconnect cause-code stats counters:

```
Router# clear h323 gateway cause-code stats

Cause code stats cleared at 01:54:08
```

In the following example from a Cisco 3640 router, the **clear h323 gateway** command is used with the **h225** keyword to clear the H.225 counters:

```
Router# show h323 gateway h225

H.225 stats cleared at 01:53:18
```

In the following example from a Cisco 3640 router, the **clear h323 gateway** command is used with the **ras** keyword to clear the RAS counters:

```
Router# clear h323 gateway ras

RAS stats cleared at 01:53:25
```

Related Commands

Command	Description
debug cch323	Provides debug output for various components within the H.323 subsystem.
show h323 gateway	Displays the statistics for H.323 gateway messages that have been sent and received and displays the reasons for which H.323 calls have been disconnected.

clear http client statistics

To reset to zero all the counters that collect the information about the communication between the HTTP server and the client displayed in the output from the **show http client statistics** command, use the **clear http client statistics** command in user EXEC or privileged EXEC mode.

clear http client statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **show http client statistics** command to display the data collected by the counters the **clear http client statistics** command resets to zero.

Examples

The following example resets the counters to zero:

```
Router# clear http client statistics
```

Related Commands

Command	Description
show http client statistics	Displays information about the communication between the HTTP server and the client.

clear interface cable-modem

To reset the controller for a specified cable modem daughter card, use the **clear interface cable-modem** command in privileged EXEC mode. This command does not have a **no** version.

clear interface cable-modem

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Examples

The following example shows how the **clear interface cable-modem** command clears the interface on the selected slot and port:

```
Router# clear interface cable-modem

*May 17 16:36:57.344: %CABLE_MODEM_HWIC-6-RESET: Interface Cable-Modem0/2/0 has been
reset: clear command
*May 17 16:37:05.348: %LINK-3-UPDOWN: Interface Cable-Modem0/2/0, changed state to down
*May 17 16:37:06.348: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable-Modem0/2/0,
changed state to down
*May 17 16:37:19.740: %LINK-3-UPDOWN: Interface Cable-Modem0/2/0, changed state to up
*May 17 16:37:27.996: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable-Modem0/2/0,
changed state to up
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured.
show interfaces cable-modem	Displays statistics for all interfaces configured on the port.

clear mgcp src-stats

To clear the statistics gathered for Media Gateway Control Protocol (MGCP) System Resource Check (SRC) Call Admission Control (CAC) on an MGCP gateway, use the **clear mgcp src-stats** command in privileged EXEC mode.

clear mgcp src-stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the **clear mgcp src-stats** command to clear the MGCP gateway buffer that holds SRC CAC statistics gathered during the most recent inspection interval.

Examples

The following example clears MGCP VoIP SRC CAC statistics:

```
Router# clear mgcp src-stats
```

Related Commands

Command	Description
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

clear mgcp statistics

To reset the Media Gateway Control Protocol (MGCP) statistical counters, use the **clear mgcp statistics** command in privileged EXEC mode.

clear mgcp statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300.
12.1(3)T	This command was implemented on the Cisco 3660, Cisco UBR924, and Cisco 2600 series.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines None

Examples The following is an example of how to enter the command:

```
Router# clear mgcp statistics
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp statistics	Displays statistics for received and transmitted packets.

clear mrcp client statistics

To clear all Media Resource Control Protocol (MRCP) statistics, use the **clear mrcp client statistics** command in privileged EXEC mode.

clear mrcp client statistics {**all** | **hostname** {*hostname* | *ip-address*}}

Syntax Description

all	Clears the accumulated MRCP session statistics for all hosts.
hostname	Clears the accumulated MRCP session statistics for the specified host.
hostname	Host name of the MRCP server. Format uses host name only or *hostname*:*port*.
ip-address	IP address of the MRCP server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command resets all MRCP session statistics to 0. Use the **show mrcp client statistics hostname** command to display the current statistics.

Examples

The following example resets the statistics for the host called “asr_server”:

```
Router# clear mrcp client statistics hostname asr_server
```

Related Commands

Command	Description
show mrcp client statistics hostname	Displays cumulative information about MRCP sessions.

clear rlm group

To reset all Redundant Link Manager (RLM) time stamps to zero, use the **clear rlm group** command in privileged EXEC mode.

clear rlm group [*group-number*] [**link** | **statistics**]

Syntax Description

group-number	(Optional) RLM group number. Range is from 0 to 255. There is no default value.
link	(Optional) Specifies the RLM group link.
statistics	(Optional) Specifies the RLM group statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **statistics** keyword was added.

Examples

The following example resets the time stamps on RLM group 1:

```
Router# clear rlm group 1 link
!
02:48:17: rlm 1: [State_Up, rx ACTIVE_LINK_BROKEN] over link [10.1.1.1(Loopback1),
10.1.4.1]
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] requests activation
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is deactivated
02:48:17: rlm 1: [State_Recover, rx LINK_BROKEN] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] = socket[10.1.1.1, 10.1.4.1]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.4.1] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is opened
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] = socket[10.1.1.2, 10.1.4.2]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.2(Loopback2),
10.1.4.2] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is opened
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] = socket[10.1.1.1, 10.1.5.1]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.5.1] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] is opened
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.5.2] = socket[10.1.1.2, 10.1.5.2]
02:48:17: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.2(Loopback2),
10.1.5.2] for user RLM_MGR
02:48:17: rlm 1: link [10.1.1.2(Loopback2), 10.1.5.2] is opened
02:48:17: rlm 1: [State_Recover, rx LINK_OPENED] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] requests activation
02:48:17: rlm 1: [State_Recover, rx LINK_OPENED] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:17: rlm 1: [State_Recover, rx START_ACK] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:17: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is activated
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (**RLM**)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (**RLM**)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
timer	Overwrites the default setting of timeout values.

clear rpms-proc counters

To clear statistics counters for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **clear rpms-proc counters** command in privileged EXEC mode.

clear rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example clears statistics counters for leg 3 AAA preauthentication requests, successes, and rejects:

```
Router# clear rpms-proc counters
```

Related Commands

Command	Description
show rpms-proc counters	Displays statistics for the number of leg 3 AAA preauthentication requests, successes, and rejects.

clear rudpv0 statistics

To clear the counters that track RUDP statistics, enter the **clear rudpv0 statistics** command in privileged EXEC mode.

clear rudpv0 statistics

Syntax Description This command has no arguments or keywords.

Command Default The statistical information accumulates.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples The following example shows how to clear RUDP statistics on a Cisco 2611 (Cisco SLT):

```
clear rudpv0 statistics
```

Related Commands

Command	Description
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them.
show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth.

clear rudpv1 statistics

To clear the counters that track Reliable User Datagram Protocol (RUDP) statistics, use the **clear rudpv1 statistics** command in privileged EXEC mode.

clear rudpv1 statistics

Syntax Description This command has no arguments or keywords.

Command Default The statistical information accumulates.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on Cisco 7200.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco IAD2420 series.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples The following example clears all RUDP statistics for all available session groups:

```
Router# clear rudpv1 statistics
```

Related Commands

Command	Description
debug rudpv1	Displays debugging information for RUDP.
show rudpv1	Displays RUDP information.

clear sccp server statistics

To clear the counts displayed under the **show sccp server statistics** command, use the **clear sccp server statistics** command in privileged EXEC mode.

clear sccp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows the Skinny Client Control Protocol (SCCP) server statistics counts being cleared, followed by verification that the counters are reset to zero with the **show sccp server statistics** command. The field descriptions are self-explanatory.

```
Router# show sccp server statistics

Failure type              Error count
------------------------  -----------
Send queue enqueue        0
Socket send               0
Msg discarded upon error  0
```

Related Commands

Command	Description
show sccp server statistics	Displays the number of SCCP messages sent and received by the SCCP server.

clear sdspfarm counters

To reset the server counts of the digital signal processor farms that are registered to the Skinny Client Control Protocol (sdspfarm) displayed under the **server show sdspfarm message statistics** command to zero, use the **clear sdspfarm counters** command in privileged EXEC mode.

clear sdspfarm counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.

Examples

The following example shows the sdspfarm counters being cleared and verification that the counters are reset to zero with the **show sdspfarm sessions state** command:

```
Router# clear sdspfarm counters

Router# show sdspfarm sessions state

Call state      Num of sessions
----------      ---------------
IDLE            1022
ALERTING        0
SEIZE           0
PROGRESS        0
CONNECTED       0
DIGITS          0
BUSY            0
RINGING         0
ERROR           0
HOLD            0
END             0
STOP            0
START           2
RESTART         0
UNKNOWN         0
DELAYED-SMT     0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show sdspfarm message statistics	Displays the number of SCCP messages sent and received by the SCCP server.
show sdspfarm sessions state	Displays the number of sessions in each SCCP call state.

clear sgcp statistics

To clear all Simple Gateway Control Protocol (SGCP) statistics, use the **clear sgcp statistics** command in privileged EXEC mode.

clear sgcp statistics

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines None

Examples The following example shows all SGCP statistics being cleared:

```
Router# clear sgcp statistics
```

Related Commands

Command	Description
show sgcp statistics	Displays global statistics for SGCP packet counts.

clear sip-ua statistics

To reset the Session Initiation Protocol (SIP) user-agent (UA) statistical counters, use the **clear sip-ua statistics** command in privileged EXEC mode.

clear sip-ua statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines Use this command to clear all SIP statistics counters that are displayed by the **show sip-ua statistics** command.

Examples The following example shows all SIP-UA statistics being cleared:

```
Router# clear sip-ua statistics
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.

clear sip-ua tcp connection

To clear a session initiation protocol (SIP) TCP connection, use the **clear sip-ua tcp connection** command in privileged EXEC mode.

clear sip-ua tcp connection {**id** *connection-id* [**target ipv4:***address***:***port*] | [**id** *connection-id*] **target ipv4:***address***:***port*}

Syntax Description

id *connection-id*	Specifies the ID of the connection that needs to be closed in the SIP TCP process. The *connection-id* argument represents the connection ID. The range is from 1 to 2048.
target ipv4:*address***:***port*	Specifies the target address for the connection that needs to be closed in the SIP transport layer.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	This command was replaced by the **clear sip-ua tcp tls connection** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua tcp connection** command can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To cear the connection entry only at the upper transport layer, assign the target IP address and port:

```
Router# clear sip-ua tcp connection target ipv4:172.18.194.183:5060
```

To clear the connection entry only at the lower TCP or User Datagram Protocol (UDP) layer, specify the connection:

```
Router# clear sip-ua tcp connection id 1
```

To completely clear a valid connection to target 172.18.194.183, port 5060, consider the following output example from the **show sip-ua connections** command:

```
Router# show sip-ua connections tcp detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua tcp connection** command:

```
Router# clear sip-ua tcp connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip tcp process
Purging the entry from reusable global connection table
```

The result is that all connections are cleared after inputting the **clear sip-ua tcp connection** command:

```
Router# show sip-ua connections tcp detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua connections	Displays SIP UA transport connection tabless.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear sip-ua tcp tls connection

To clear a session initiation protocol (SIP) TCP connection, use the **clear sip-ua tcp tls connection** command in privileged EXEC mode.

clear sip-ua tcp tls connection {**id** *connection-id* [**target ipv4:***address***:***port*] | [**id** *connection-id*] **target ipv4:***address***:***port*}

Syntax Description

id *connection-id*	Specifies the ID of the connection that needs to be closed in the SIP TCP process. The *connection-id* argument represents the connection ID. The range is from 1 to 2048.
target ipv4:*address***:***port*	Specifies the target address for the connection that needs to be closed in the SIP transport layer.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introducted to replace the **clear sip-ua tcp connection** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua tcp tls connection** command can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To cear the connection entry only at the upper transport layer, assign the target IP address and port:

```
Router# clear sip-ua tcp tls connection target ipv4:172.18.194.183:5060
```

To clear the connection entry only at the lower TCP or User Datagram Protocol (UDP) layer, specify the connection:

```
Router# clear sip-ua tcp tls connection id 1
```

To completely clear a valid connection to target 172.18.194.183, port 5060, consider the following output example from the **show sip-ua connections** command:

```
Router# show sip-ua connections tcp tls detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua tcp connection** command:

```
Router# clear sip-ua tcp tls connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip tcp process
Purging the entry from reusable global connection table
```

The result is that all connections are cleared after inputting the **clear sip-ua tcp connection** command:

```
Router# show sip-ua connections tcp tls detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua connections	Displays SIP UA transport connection tabless.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear sip-ua udp connection

To clear a SIP UDP connection, use the **clear sip-ua udp connection** command in privileged EXEC mode.

clear sip-ua udp connection {**id** *value* [**target** *ip-address*] | [**id** *value*] **target** *ip-address*}

Syntax Description

id *value*	Specifies the ID of the connection that needs to be closed in the SIP UDP process. The *value* argument represents the value of the connection ID. The range is from 1 to 2048.
target ip-address	Specifies the target address for the connection that needs to be closed in the SIP transport layer. The *ip-address* argument is the target address in the form of **ipv4:***address***:***port*.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Inappropriate usage of the **clear sip-ua udp connection** command without understanding the issue or the implications can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To purge the connection entry only at the upper transport layer, assign the target IP address and port.

```
Router# clear sip-ua udp connection target ipv4:172.18.194.183:5060
```

To purge the connection entry only at the lower TCP/UDP layer, assign the connection ID.

```
Router# clear sip-ua udp connection id 1
```

Note Inappropriate usage of the **clear** command without understanding the issue or the implications would lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

To completely purge a valid connection to target 172.18.194.183, port 5060, consider the following example.

Before executing the **clear sip-ua udp connection** command, running the **show sip-ua connections** command gave the following output.

```
Router# show sip-ua connections udp detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
```

```
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua udp connection** command:

```
Router# clear sip-ua udp connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip udp process
Purging the entry from reusable global connection table
```

The final result is that all connections are cleared after executing the **clear sip-ua udp connection** command:

```
Router# show sip-ua connections udp detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua tcp connection	Clears a SIP TCP connection.
show sip-ua connections	Displays SIP UA transport connections.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear ss7 sm-stats

To clear the counters that track session manager statistics, use the **clear ss7 sm-stats** command in privileged EXEC mode.

clear ss7 sm-stats [**session-set** *number*]

Syntax Description

session-set	(Optional) Specifies the session set.
number	(Optional) Specifies the session-set number. The range is from 0 to 3.

Command Default The statistical information accumulates.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **session-set** keyword and *number* argument were added.

Examples The following example shows how to clear session manager statistics:

```
Router# clear ss7 sm-stats session-set 2
```

Related Commands

Command	Description
show ss7 sm stats	Displays session manager information about number of packets queued, received, and so forth.

clear statistics dial-peer voice

To reset voice call counters and recent call details stored in a dial peer, use the **clear statistics dial-peer voice** command in privileged EXEC mode.

clear statistics dial-peer voice [*tag*| **busy-trigger-counter**]

Syntax Description

tag	(Optional) Identification tag number of a specific dial peer. A valid entry is any integer that identifies a specific dial peer. Range is from 1 to 2147483647.
busy-trigger-counter	(Optional) Specifies to clear the dial peer busy trigger call counter.

Command Default

If the *tag* argument is not used, counters in all the configured voice dial peers are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco AS5300.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **busy-trigger-counter** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **clear statistics dial-peer voice** command resets the following statistical information about calls:

- Time elapsed since last clearing of statistics
- Connect time
- Charged units
- Accepted calls
- Refused calls
- Successful calls
- Failed calls
- Incomplete calls
- Last disconnect cause
- Last disconnect text
- Last setup time

Examples

The following example shows how to clear voice dial peer statistics using tag 1234:

```
Router# clear statistics dial-peer voice 1234
Clear voice call statistics stored in this voice dial-peer [confirm]y
```

The following example shows how to clear statistics in all the configured voice dial peers:

```
Router# clear statistics dial-peer voice

Clear voice call statistics stored in all voice dial-peers [confirm]y
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
show call history voice record	Displays CDR events in the call history table.
show dial-peer voice	Displays configuration information for dial peers.

clear stcapp statistics

To clear SCCP Telephony Control Application (STCAPP) statistics, use the **clear stcapp statistics** command in privileged EXEC mode.

clear stcapp statistics {**all** | **port** *slot-number*}

Syntax Description

all	Clears all STCAPP statistics.
port	Clears port-level STCAPP statistics.
slot-number	Voice interface slot number. The range is from 0 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example show how to clear all STCAPP statistics:

```
Router# clear stcapp statistics all
```

Related Commands

Command	Description
stcapp	Enables the STCAPP.

clear subscription

To clear all active subscriptions or a specific subscription, use the **clear subscription** command in privileged EXEC mode.

clear subscription {**all** | **session-id** *session-id* | **statistics**}

Syntax Description

all	All active subscriptions.
session-id *session-id*	Subscription session to be cleared.
statistics	Global subscription statistics and all subscription history records.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines To cancel a specific subscription, use the *session-id* argument. You can obtain the session ID by viewing **show subscriptions** output. When this command is used, the applications associated with subscriptions receive the ev_subscribe_cleanup event. On receiving this event, the script closes the subscription.

Examples The following example shows global statistics and history records being cleared:

```
Router# clear subscription statistics
```

Related Commands

Command	Description
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
show subscription sip	Displays active SIP subscriptions.
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by the gateway.

clear tgrep counters

To clear Telephony Gateway Registration Protocol (TGREP) counters, use the **clear tgrep counters** command in privileged EXEC mode.

clear tgrep counters {***** | **carrier** *string* | **csr** | **dial-peer** *tag* | **trunk-group** *label*} [**csr**] [**ac**]

Syntax Description

*****	Clears all TGREP counters.
carrier	Clears available circuit counters.
string	Carrier ID.
dial-peer	Clears dial-peer.
tag	Dial peer tag. The range is from 1 to 2147483647.
trunk-group *label*	Clears the trunk-group counters.
csr	(Optional) Clears the call success rate counters.
ac	(Optional) Clears all the available circuit counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example show how to clear all tgrep counter information:

```
Router# clear tgrep counters *
```

Related Commands

Command	Description
clear tgrep neighbor	Clears all neighbor sessions.

clear tgrep neighbor

To clear Telephony Gateway Registration Protocol (TGREP) neighbor sessions, use the **clear tgrep neighbor** command in privileged EXEC mode.

clear tgrep neighbor {***** | *ip-address*}

Syntax Description

*****	Clears all neighbor sessions.
ip-address	IP addresses of neighbor sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to clear neighbor sessions:

```
Router# clear tgrep neighbor *
```

Related Commands

Command	Description
clear tgrep counters	Clears TGREP counters.

clear voice accounting method

To clear VoIP AAA accounting statistics for a specific accounting method on the gateway, use the **clear voice accounting method** command in privileged EXEC mode.

clear voice accounting method *method-list-name*

Syntax Description

method-list-name	Name of the method list.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example clears accounting statistics for method list “h323”:

```
Router# clear voice accounting method h323
```

Related Commands

Command	Description
voice statistics type csr	Configures the collection of signaling and VoIP AAA accounting statistics.

clear voice dsp

To "cold-start" one or more digital signal processor (DSP) voice channels, use the **clear voice dsp** command in privileged EXEC mode.

clear voice dsp {**channels** | **error**} [*slot*[*/dsp*][*/channel*]] [*slot*[*/dsp*][*/channel*]]

Syntax Description

channels	Clears DSP calls on a specific channel or a range of channels.
error	Clears DSP error statistics.
slot	(Optional) Specifies either a single slot or the first slot in a range. To specify a range of slots, you can enter a **second slot in the syntax of this argument. The second slot specifies the end of the range.** All slots in the range are affected by the command.
/dsp	(Optional) Specifies either a single DSP on the slot or the first DSP in a range. To specify a range of DSPs, you can enter a **second DSP in the syntax of this argument. The second DSP specifies the end of the range.** All DSPs in the range are affected by the command.
/channel	(Optional) Specifies either a single channel on the DSP or the first channel in a range. To specify a range of channels, you can enter a **second channel in the syntax of this argument. The second channel specifies the end of the range.** All channels in the range are affected by the command.

Command Default

If this command is not used, active calls continue on the DSP voice channels.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **clear voice dsp** command allows you to cold-start DSPs. Execution of this command causes the configured firmware to be downloaded to the specified DSP or a range of DSPs. This command can be executed irrespective of the state of the DSPs. All the active channels of the DSPs are prematurely terminated.

Examples

The following example clears all active calls on slot 2, DSP 1:

```
Router# clear voice dsp 2/1
```

The following example clears the active calls on slot 2, DSP 1, channel 1:

```
Router# clear voice dsp 2/1/1
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels

clear voice statistics

To clear voice-statistic collection settings on the gateway to reset the statistics collection, use the **clear voice statistics** command in privileged EXEC mode.

clear voice statistics [**csr** [**accounting** | **signaling**]] | [**iec**]

Syntax Description

csr	(Optional) All accounting and signaling statistics are cleared, but Cisco VoIP internal error codes (IECs) are not cleared.
accounting	(Optional) Only accounting statistics are cleared.
signaling	(Optional) Only signaling statistics are cleared.
iec	(Optional) Only Cisco VoIP IECs are cleared.

Command Default

If no keywords are specified, all accounting and signaling statistics, and all IECs are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example clears all accounting and signaling statistics, and all Cisco VoIP IECs:

```
Router# clear voice statistics
```

The following example clears all accounting and signaling statistics:

```
Router# clear voice statistics csr
```

The following example clears only accounting statistics:

```
Router# clear voice statistics csr accounting
```

The following example clears only signaling statistics:

```
Router# clear voice statistics csr signaling
```

The following example clears only Cisco VoIP IECs:

```
Router# clear voice statistics iec
```

Related Commands

Command	Description
voice statistics type csr	Configures the collection of signaling and VoIP AAA accounting statistics.

clear vsp statistics

To clear all Voice Streaming Processing (VSP) statistics that are displayed when using the **show vsp** command is used, use the **clear vsp statistics** command in privileged EXEC mode.

clear vsp statistics

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines This command resets all cumulative VSP statistics to 0. Use the **show vsp statistics** command to display the current statistics.

Examples The following example resets the statistics for VSP sessions:

```
Router# clear vsp statistics
```

Related Commands

Command	Description
show vsp	Displays cumulative information about VSP sessions.

clid

To preauthenticate calls on the basis of the Calling Line Identification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

no clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **ctype** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
 group radius
 clid required
```

Related Commands

Command	Description
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

clid (dial peer)

To control the presentation and use of calling-line ID (CLID) information, use the **clid** command in dial peer configuration mode. To remove CLID controls, use the **no** form of this command.

clid {**network-number** *number* [**second-number** strip] | **network-provided** | **override rdnis** | **restrict** | **strip** [**name** | **pi-restrict** [**all**]] | **substitute name**}

no clid {**network-number** *number* [**second-number** strip] | **network-provided** | **override rdnis** | **restrict** | **strip** [**name** | **pi-restrict** [**all**]] | **substitute name**}

Syntax Description

network-number *number*	Network number. Establishes the calling-party network number in the CLID for this router.
network-provided	Allows you to set the screening indicator to reflect the number that was provided by the network.
override rdnis	Supported for POTS dial peers only Overrides the CLID with the redirected dialed number identification service (RDNIS) if available.
pi-restrict	Restricted progress indicator (PI). Causes removal of the calling-party number from the CLID when the PI is restricted.
restrict	Restricts presentation of the caller ID in the CLID.
second-number strip	(Optional) Removes a previously configured second network number from the CLID.
strip	Strips the calling-party number from the CLID. • **name**—(Optional) Calling-party name. Causes removal of the calling-party name from the CLID. • **pi-restrict** [**all**]—(Optional) Restricted PI. Causes removal of all calling-party names and numbers from the CLID when the PI is restricted.
substitute name	Copies the calling number into the display name if PI allows it (and the calling name is empty).

Command Default

No default behavior or values

Command Modes

Dial Peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **override rdnis** keywords were added.
12.4(4)T	The following keywords were added: **network-provided**, **pi-restrict all**, and **substitute name**.

Usage Guidelines

The **override rdnis** keywords are supported only for POTS dial peers.

CLID is the collection of information about the billing telephone number from which a call originated. The CLID value might be the entire phone number, the area code, or the area code plus the local exchange. It is also known as caller ID. The various keywords to this command manage the presentation, restriction, or stripping of the various CLID elements.

The **clid network-number** command sets the presentation indicator to "y" and the screening indicator to "network-provided." The **second-number strip** keyword strips from the H.225 source-address field the original calling-party number, and is valid only if a network number was previously configured.

The **clid override rdnis** command overrides the CLID with the RDNIS if it is available.

The **clid restrict** command causes the calling-party number to be present in the information element, but the presentation indicator is set to "n" to prevent its presentation to the called party.

The **clid strip** command causes the calling-party number to be null in the information element, and the presentation indicator is set to "n" to prevent its presentation to the called party.

Examples

The following example sets the calling-party network number to 98765 for POTS dial peer 4321:

```
Router(config)# dial-peer voice 4321 pots
Router(config-dial-peer)# clid network-number 98765
```

An alternative method of accomplishing this result is to enter the **second-number strip** keywords as part of the **clid network-number** command. The following example sets the calling-party network number to 56789 for VoIP dial peer 1234 and also prevents the second network number from being sent:

```
Router(config)# dial-peer voice 1234 voip
Router(config-dial-peer)# clid network-number 56789 second-number strip
```

The following example overrides the calling-party number with RDNIS if available:

```
Router(config-dial-peer)# clid override rdnis
```

The following example prevents the calling-party number from being presented:

```
Router(config-dial-peer)# clid restrict
```

The following example removes the calling-party number from the CLID information and prevents the calling-party number from being presented:

```
Router(config-dial-peer)# clid strip
```

The following example strips the name from the CLID information and prevents the name from being presented:

```
Router(config-dial-peer)# clid strip name
```

The following example strips the calling party number when PI is set to restrict clid strip from the CLID information and prevents the calling party number from being presented:

```
Router(config-dial-peer)# clid strip pi-restrict
```

The following example strips calling party name and number when the PI is set to the restrict all clid strip from the CLID information and prevents the calling party name and number from being presented:

```
Router(config-dial-peer)# clid strip pi-restrict all
```

The following example substitutes the calling party number into the display name:

```
Router(config-dial-peer)# clid substitute name
```

The following example allows you to set the screening indicator to reflect that the number was provided by the network:

```
Router(config-dial-peer)# clid network-provided
```

Related Commands

Command	Description
clid (voice-service-voip)	Passes the network provided ISDN numbers in an ISDN calling party information element screening indicator field, removes the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allows a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers.

clid (voice-service-voip)

To pass the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and remove the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allow a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers use the **clid** command in voice service voip configuration mode. To return to the default configuration, use the **no** form of this command.

clid {**network-provided | strip pi-restrict all | substitute name**}

no clid {**network-provided | strip pi-restrict all | substitute name**}

Syntax Description

network-provided	Sets the screen indicator as network-provided.
strip pi-restrict all	Removes the CLID when the progress indicator (PI) is restricted for PSTN to SIP operations and removes the calling party name and number when the PI is restricted for PSTN to SIP operations.
substitute name	Copies the calling number to the display name if unavailable for PSTN to SIP operations.

Command Default

The **clid** command passes along user-provided ISDN numbers in an ISDN calling party information element screening indicator field.

Command Modes

Voice-service-VoIP configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **clid network-provided** keyword to pass along network-provided ISDN numbers in an ISDN calling party information element screening indicator field.

Use the **clid strip pi-restrict all** keyword to remove the Calling Party Name and Calling Party Number from the CLID.

Use the **clid substitute name** keyword to allow a presentation of the Display Name field in the Remote-Party-ID and From headers. The Calling Number is substituted for the Display Name field.

Examples

The following example passes along network-provided ISDN numbers in an ISDN calling party information element screening indicator field:

```
Router(conf-voi-serv)# clid network-provided
```

The following example passes along user-provided ISDN numbers in an ISDN calling party information element screening indicator field:

```
Router(conf-voi-serv)# no clid network-provided
```

The following example removes the calling party name and number from the calling-line identifier (CLID):

```
Router(conf-voi-serv)# clid strip pi-restrict all
```

The following example does not remove the calling party name and number from the CLID:

```
Router(conf-voi-serv)# no clid strip pi-restrict all
```

The following example allows the presentation of the calling number to be substituted for the missing Display Name field in the Remote-Party-ID and From headers:

```
Router(conf-voi-serv)# clid substitute name
```

The following example disallows the presentation of the calling number to be substituted for the missing Display Name field in the Remote-Party-ID and From headers:

```
Router(conf-voi-serv)# no clid substitute name
```

Related Commands

Command	Description
clid (dial-peer)	Controls the presentation and use of CLID information in dial peer configuration mode.

clid strip

To remove the calling-party number from calling-line-ID (CLID) information and to prevent the calling-party number from being presented to the called party, use the **clid strip** command in dial peer configuration mode. To remove the restriction, use the **no** form of this command.

clid strip [**name**]

no clid strip [**name**]

Syntax Description

name	(Optional) Removes the calling-party name for both incoming and outgoing calls.

Command Default

Calling-party number and name are included in the CLID information.

Command Modes

Dial peer configuration

Command History

Cisco IOS Release	Cisco CME Version	Modification
12.2(11)T	2.01	This command was introduced.
12.2(15)ZJ1	3.0	The **name** keyword was added.
12.3(4)T	3.0	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

If the **clid strip** command is issued, the calling-party number is null in the information element, and the presentation indicator is set to "n" to prevent the presentation of the number to the called party.

If you want to remove both the number and the name, you must issue the command twice, once with the **name** keyword.

Examples

The following example removes the calling-party number from the CLID information and prevents the calling-party number from being presented:

```
Router(config-dial-peer)# clid strip
```

The following example removes both the calling-party number and the calling-party name from the caller-ID display:

```
Router(config-dial-peer)# clid strip
Router(config-dial-peer)# clid strip name
```

Related Commands

Command	Description
clid network-number	Configures a network number in the router for CLID and uses it as the calling-party number.
clid restrict	Prevents the calling-party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.

clid strip reason

To remove the calling-line ID (CLID) reason code and to prevent it from being displayed on the phone, use the **clid strip reason** command in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

clid strip reason

no clid strip reason

Syntax Description

This command has no arguments or keywords.

Command Default

The CLID reason code is not removed.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

When the **caller-id enable** command is enabled on the gateway so that the gateway forwards information depending on the preference of the caller, client layer interface port (CLIP), or calling line identification restriction (CLIR), an "unavailable" message is displayed on the terminating phone. An "unavailable" message is a standard message that indicates the reason for the absence of calling party name.

You can use the **clid strip reason** command to remove the message and have only the call parameters forwarded.

Examples

The following example shows how to remove the CLID reason code:

```
Router# configure terminal
Router(config)# dial-peer voice 88 voip
Router(config-dial-peer)# clid strip reason
```

Related Commands

Command	Description
caller-id enable	Allows the sending or receiving of caller-ID information.
clid strip	Removes the calling-party number from CLID information and prevents the calling-party number from being presented to the called party.
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

clock-rate (codec-profile)

To set the clock rate, in Hz, for the codec, use the **clock-rate** command in codec-profile configuration mode. To return to the default value, use the **no** form of this command.

clock-rate *clock-rate*

no clock-rate

Syntax Description

clock-rate	Number in the range of 1 to 1000000.

Command Default

The default clock rate is 0.

Command Modes

Codec-profile configuration (config-codec-profile)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

The clock-rate must be set to 90000 for H.263/H.264.

Examples

The following example shows:

```
codec profile 116 h263
    clock-rate 500000
    fmtp "fmtp "fmtp:120 SQCIF=1;QCIF=1;CIF=1;CIF4=2;MAXBR=3840;I=1""
!
```

Related Commands

Command	Description
codec profile	Defines video capabilities needed for video endpoints.

clock-select

To establish the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module, use the **clock-select** command in CES configuration mode.

clock-select *priority-number interface slot/port*

Syntax Description

priority-number	Priority of the clock source. Range is from 1 (high priority) to 4 (low priority). There is no default value.
interface	Specifies the interface to supply the clock source.
slot/port	Backplane slot number and port number on the interface.

Command Default

No default behavior or values

Command Modes

CES configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

This command is used on Cisco 3600 series routers that have OC-3/STM-1 ATM CES network modules.

To support synchronous or synchronous residual time stamp (SRTS) clocking modes, you must specify a primary reference source to synchronize the flow of constant bit rate (CBR) data from its source to its destination.

You can specify up to four clock priorities. The highest priority active interface in the router supplies primary reference source to all other interfaces that require network clock synchronization services. The fifth priority is the local oscillator on the network module.

Use the **show ces clock-select** command to display the currently configured clock priorities on the router.

Examples

The following example defines two clock priorities on the router:

```
clock-select 1 cbr 2/0
clock-select 2 atm 2/0
```

Related Commands

Command	Description
channel-group	Configures the timing recovery clock for the CES interface.
clock source	Configures a transmit clock source for the CES interface.
show ces clock	Displays which ports are designated as network clock sources.

codec (dial peer)

To specify the voice coder rate of speech for a dial peer, use the **codec** command in dial peer voice configuration mode. To reset command settings to the default value, use the **no** form of this command.

Cisco 1750 and Cisco 1751 Modular Access Routers, Cisco AS5300 and AS5800 Universal Access Servers, and Cisco MC3810 Multiservice Concentrators

codec *codec* [**bytes** *payload-size*] [**fixed-bytes**] [**mode** {**independent** | **adaptive**} [**bit-rate** *value*] [**framesize** {**30** | **60**} [**fixed**]]

no codec *codec* [**bytes** *payload-size*] [**fixed-bytes**] [**mode** {**independent** | **adaptive**} [**bit-rate** *value*] [**framesize** {**30** | **60**} [**fixed**]]

Cisco 2600, 3600, 7200, and 7500 Series Routers

codec {*codec* [**bytes** *payload-size*] | **transparent**} [**fixed-bytes**] [**mode** {**independent** | **adaptive**} [**bit-rate** *value*] [**framesize** {**30** | **60**} [**fixed**]]

no codec {*codec* [**bytes** *payload-size*] | **transparent**} [**fixed-bytes**] [**mode** {**independent** | **adaptive**} [**bit-rate** *value*] [**framesize** {**30** | **60**} [**fixed**]]

Syntax Description

codec	Specifies the voice coder rate for speech. Codec options available for various platforms are described in Table 11.
bytes	(Optional) Precedes the argument that specifies the number of bytes in the voice payload of each frame.
payload-size	(Optional) Number of bytes in the voice payload of each frame. See Table 12 for valid entries and default values.
transparent	Enables codec capabilities to be passed transparently between endpoints in a Cisco Unified Border Element. **Note** The **transparent** keyword is available only on the Cisco 2600, 3600, 7200, and 7500 series router platforms.
fixed-bytes	(Optional) Indicates that the codec byte size is fixed and non-negotiable.
mode	(Optional) For iSAC codec only. Specifies the iSAC operating frame mode that is encapsulated in each packet.
independent | **adaptive**	(Optional) For iSAC codec only. Determines whether configuration mode (VBR) is **independent** (value 1) or **adaptive** (value 0).
bit rate *value*	(Optional) For iSAC codec only. Configures the target bit rate. The range is 10 to 32 kbps.
frame-size	(Optional) For iSAC codec only. Specifies the operating frame in milliseconds (ms). Valid entries are: • **30**—30-ms frames • **60**—60-ms frames • **fixed**—This keyword is applicable only for adaptive mode.

Command Default

g729r8, 30-byte payload for VoFR and VoATM.
g729r8, 20-byte payload for VoIP.
See Table 12 for valid entries and default values for codecs.

Command Modes

Dial peer configuration (config-dialpeer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(3)T	This command was implemented on the Cisco 2600 series.
12.0(3)T	This command was implemented on the Cisco AS5300. This release does not support the **clear-channel** keyword.
12.0(4)T	This command was implemented on the Cisco 3600 series, Cisco 7200 series, and Cisco MC3810, and the command was modified for VoFR dial peers.
12.0(5)XE	Additional *codec* choices and other options were implemented.
12.0(5)XK	The **g729br8** and **pre-ietf** codec choices were added for the Cisco 2600 and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0.(7)T and implemented on the Cisco AS5800. Voice coder rates of speech were added. This release does not support the **clear-channel** keyword were added on this platform.
12.0(7)XK	**g729abr8** and **g729ar8** codec choices were for the Cisco MC3810, and the keyword **pre-ietf** was deleted.
12.1(1)T	This command was integrated in Cisco IOS Release 12.1(1)T.
12.1(5)T	**gsmefr** and **gsmfr** codec keywords were added.
12.2(8)T	The command was implemented on the Cisco 1750 and Cisco 1751.
12.2(13)T3	The **transparent** keyword was added for use with H.323 to H.323 connections. This keyword is available only in js2 images.
12.4(11)XJ2	**gsmefr** and **gsmfr** keywords were removed as configurable codec options for all platforms with the exception of the **gsmfr** codec on the Cisco AS5400 and AS5350 with MSAv6 DSPs. The **transparent** keyword now supports H.323 to SIP connections.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(15)XY	The **g722-64** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)M	The **fixed-bytes** keyword was added.
15.1(1)T	This command was modified. The **isac** keyword was added as a codec type, and the **mode**, **independent**, **adaptive**, **bit rate**, and **fixed** keywords were added as configurable parameters.

Usage Guidelines

Use this command to define a specific voice coder rate of speech and payload size for a VoIP or VoFR dial peer. This command is also used for VoATM.

Table 11 Codec Support by Platform

Codec	Cisco 1750 and Cisco 1751 Modular Access Routers	Cisco 2600 and 3600 Series Routers and Cisco 7200 and 7500 Series Routers	Cisco AS5300 and AS5800 Universal Access Servers	Cisco MC3810 Multiservice Concentrators
clear-channel—Clear channel at 64,000 bits per second (bps)	Yes	Yes	—	Yes
g711alaw—G.711 A-Law at 64,000 bps	Yes	Yes	Yes	Yes
g711ulaw—G.711 mu-Law at 64,000 bps	Yes	Yes	Yes	Yes
g722-64—G.722-64 at 64,000 bps	Yes	Yes	Yes	—
g723ar53—G.723.1 Annex A at 5300 bps	—	Yes	Yes	Yes
g723ar63—G.723.1 Annex A at 6300 bps	—	Yes	Yes	Yes
g723r53—G.723.1 at 5300 bps	—	Yes	Yes	Yes
g723r63—G.723.1 at 6300 bps	—	Yes	Yes	Yes
g726r16—G.726 at 16,000 bps	Yes	Yes	Yes	Yes
g726r24—G.726 at 24,000 bps	Yes	Yes	Yes	Yes
g726r32—G.726 at 32,000 bps	Yes	Yes	Yes	Yes
g726r53—G.726 at 53,000 bps	Yes	Yes	Yes	—
g726r63—G.726 at 63,000 bps	Yes	Yes	Yes	—
g728—G.728 at 16,000 bps	—	Yes	Yes	Yes
g729abr8—G.729 Annex A and B at 8000 bps	Yes	Yes	Yes	Yes
g729ar8—G.729 Annex A at 8000 bps	Yes	Yes	Yes	Yes
g729br8—G.729 Annex B at 8000 bps	Yes	Yes	Yes	Yes
g729r8—G.729 at 8000 bps. This is the default codec.	Yes	Yes	Yes	Yes
isac—Cisco internet Speech Audio Codec (iSAC) codec.	Yes	Yes	Yes	Yes

A specific codec type can be configured on the dial peer as long as the codec is supported by the setting used with the **codec complexity** voice-card configuration command. The **codec complexity** command is voice-card specific and platform specific. The **codec complexity** voice-card configuration command is set to either high or medium.

If the **codec complexity** command is set to high, the following keywords are available: **g711alaw**, **g711ulaw**, **g722-64**, **g723ar53**, **g723ar63**, **g723r53**, **g723r63**, **g726r16**, **g726r24**, **g726r32**, **g728**, **g729r8**, and **g729br8**.

If the **codec complexity** command is set to medium, the following keywords are available: **g711alaw**, **g711ulaw**, **g726r16**, **g726r24**, **g726r32**, **g729r8**, and **g729br8**.

The **codec** dial peer configuration command is particularly useful when you must change to a small-bandwidth codec. Large-bandwidth codecs, such as G.711, do not fit in a small-bandwidth link. However, the g711alaw and g711ulaw codecs provide higher quality voice transmission than other codecs. The g729r8 codec provides near-toll quality with considerable bandwidth savings.

The **transparent** keyword is available with H.323 to H.323 call connections beginning in Cisco IOS Release 12.2(13)T3. Support for the keyword in H.32 to SIP call connections begins in Cisco IOS Release 12.4(11)XJ2.

If codec values for the dial peers of a connection do not match, the call fails.

You can change the payload of each VoIP frame by using the **bytes** keyword; you can change the payload of each VoFR frame by using the **bytes** keyword with the *payload-size* argument. However, increasing the payload size can add processing delay for each voice packet.

Table 12 describes the voice payload options and default values for the codecs and packet voice protocols.

Table 12 Voice Payload-per-Frame Options and Defaults

Codec	Protocol	Voice Payload Options (in Bytes)	Default Voice Payload (in Bytes)
g711alaw **g711ulaw**	VoIP VoFR VoATM	80, 160 40 to 240 in multiples of 40 40 to 240 in multiples of 40	160 240 240
g722-64	VoIP	80, 160, 240	160
g723ar53 **g723r53**	VoIP VoFR VoATM	20 to 220 in multiples of 20 20 to 240 in multiples of 20 20 to 240 in multiples of 20	20 20 20
g723ar63 **g723r63**	VoIP VoFR VoATM	24 to 216 in multiples of 24 24 to 240 in multiples of 24 24 to 240 in multiples of 24	24 24 24
g726r16	VoIP VoFR VoATM	20 to 220 in multiples of 20 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g726r24	VoIP VoFR VoATM	30 to 210 in multiples of 30 15 to 240 in multiples of 15 30 to 240 in multiples of 15	60 90 90
g726r32	VoIP VoFR VoATM	40 to 200 in multiples of 40 20 to 240 in multiples of 20 40 to 240 in multiples of 20	80 120 120
g728	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g729abr8 **g729ar8** **g729br8** **g729r8**	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	20 30 30
isac	VoIP	10 to 230 in multiples of 10	30 60

Note If you are configuring G.729r8 or G.723 as the *codec-type*, the maximum value for the *payload-size* argument is 60 bytes.

For toll quality, use the **g711alaw** or **g711ulaw** keyword. These values provide high-quality voice transmission but use a significant amount of bandwidth. For nearly toll quality (and a significant savings in bandwidth), use the **g729r8** keyword.

Note The G.723 and G.728 codecs are not supported on the Cisco 1700 platform for Cisco Hoot and Holler applications.

Note The **clear-channel** keyword is not supported on the Cisco AS5300.

Note The G.722-64 codec is supported only for H.323 and SIP.

Examples

The following example shows how to configure a voice coder rate that provides toll quality voice with a payload of 120 bytes per voice frame on a router that acts as a terminating node. The sample configuration begins in global configuration mode and is for VoFR dial peer 200.

```
dial-peer voice 200 vofr
 codec g711ulaw bytes 240
```

The following example shows how to configure a voice coder rate for VoIP dial peer 10 that provides toll quality but uses a relatively high amount of bandwidth:

```
dial-peer voice 10 voip
 codec g711alaw
```

The following example shows how to configure the transparent codec used by the Cisco Unified Border Element:

```
dial-peer voice 1 voip
 incoming called-number .T
 destination-pattern .T
 session target ras
 codec transparent
```

Related Commands

Command	Description
codec (DSP interface dsp farm)	Specifies call density and codec complexity.
codec (voice port)	Specifies voice compression.
codec complexity	Specifies call density and codec complexity based on the codec used.
show dial peer voice	Displays the codec setting for dial peers.

codec (dsp)

To specify call density and codec complexity based on a particular codec standard, use the **codec** command in DSP interface DSP farm configuration mode. To reset the card type to the default, use the **no** form of the command.

codec {**high** | **med**}

no codec {**high** | **med**}

Syntax Description

high	Specifies high complexity: two channels of any mix of codec.
med	Specifies medium complexity: four channels of g711/g726/g729a/fax.

Command Default Medium complexity

Command Modes DSP interface DSP farm

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.1(1)T	This command was integrated into Cisco Release 12.1(1)T.
12.1(3)T	This command was implemented on the Cisco 7500 series.

Usage Guidelines This command is supported on only the Cisco 7200 series and Cisco 7500 series routers.

Codec complexity refers to the amount of processing required to perform compression. Codec complexity affects the number of calls, referred to as call density, that can take place on the DSPfarm interfaces. The greater the codec complexity, the fewer the calls that are handled. For example, G.711 requires less DSP processing than G.728, so as long as the bandwidth is available, more calls can be handled simultaneously by using the G.711 standard than by using G.728.

The DSPinterface dspfarm **codec** complexity setting affects the options available for the **codec** dial peer configuration command.

To change codec complexity, you must first remove any configured channel associated signaling (CAS) or DS0 groups and then reinstate them after the change.

Note On the Cisco 2600 series routers, and 3600 series codec complexity is configured using the **codec complexity** command in voice-card configuration mode.

Examples The following example configures the DSPfarm interface 1/0 on the Cisco 7200 series routers to support high compression:

```
dspint DSPFarm 1/0
 codec high
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice codec rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard you are using.

codec (DSP farm profile)

To specify the codecs that are supported by a digital signal processor (DSP) farm profile, use the **codec** command in DSP farm profile configuration mode. To remove the codec, use the **no** form of this command.

codec {*codec-type* [*resolution*] | [**frame-rate** *framerate*] | [**bitrate** *bitrate*] | [**rfc-2190**] | **pass-through**}

no codec {*codec-type* [*resolution*] | [**frame-rate** *framerate*] | [**bitrate** *bitrate*] | [**rfc-2190**] | **pass-through**}

Syntax Description

codec-type	Specifies the codec preferred. • **g711alaw**—G.711 a-law 64,000 bits per second (bps) • **g711ulaw**—G.711 mu-law 64,000 bps • **g722r-64**—G.722-64 at 64,000 bps • **g729abr8**—G.729 ANNEX A and B 8000 bps • **g729ar8**—G.729 ANNEX A 8000 bps • **g729br8**—G.729 ANNEX B 8000 bps • **g729r8**—G.729 8000 bps • **h263**—H.263 video codec • **h264**—H.264 video codec • **ilbc**—Internet Low Bitrate Codec (iLBC) • **isac**—Cisco internet Speech Audio Codec (iSAC) codec
resolution	Specifies the supported video resolution. The valid entries are: • For H.263—**qcif** and **cif** • For H.264—**qcif**, **cif, vga, w360p**, **w448p, 4cif,** and **720p** **Note** 720p option applies only to homogeneous video conferences.
frame-rate *framerate*	Specifies the frame rate. The valid entries are 15 fps or 30 fps. This option applies to homogeneous conferences only.
bitrate *bitrate*	Specifies the bitrate. This option applies to homogeneous conferences only.
rfc-2190	Specifies the payload format follow RFC-2190.
pass-through	Enables codec pass-through. Supported for transcoding and media termination point (MTP) profiles.

Command Default

The following transcoding default apply when you are configuring audio profiles only. When you configure video transcoding, you must specify the audio codecs.

Transcoding

- **g711alaw**

- **g711ulaw**
- **g729abr8**
- **g729ar8**

Conferencing

- **g711alaw**
- **g711ulaw**
- **g729abr8**
- **g729ar8**
- **g729br8**
- **g729r8**

MTP

- **g711ulaw**

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(4)T	The **pass-through** keyword was added.
12.4(11)XJ2	The **gsmefr** and **gsmfr** keywords were removed as configurable codec options for all platforms.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(15)XY	The **g722r-64** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.1(1))T	This command was modified. The **isac** keyword was added.
15.1(4)M	This command was modified. The **frame-rate, bitrate, rfc-2190, and pass-through** keywords were added and codec support was added for **ilbc**, **h.263** and **h.264**.

Usage Guidelines

Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

For homogeneous video profiles, only one video format is supported

For heterogeneous and heterogeneous guaranteed-audio video profiles, multiple video formats and audio codecs are supported.

To change the configured codec in the profile, you must first enter a **no maximum session** command.

Table 13 shows the relationship between DSP farm functions and codecs.

Table 13 DSP Farm Functions and Codec Relationships

DSP Farm Function	Supported Codec
Transcoding	• **g711alaw** • **g711ulaw** • **g729abr8** • **g729ar8** • **iSAC** • **h263** • **h264**
Conferencing	• **g711alaw** • **g711ulaw** • **g722r-64** • **g729abr8** • **g729ar8** • **g729br8** • **g729r8** • **h263** • **h264** • **ilbc**
MTP	• **g711ulaw** • **iSAC**

Hardware MTPs support only G.711 a-law and G.711 mu-law. If you configure a profile as a hardware MTP and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command.

The **pass-through** keyword is supported for transcoding and MTP profiles only; the keyword is not supported for conferencing profiles. To support the Resource Reservation Protocol (RSVP) agent on a Skinny Client Control Protocol (SCCP) device, you must use the **codec pass-through** command. In the pass-through mode, the SCCP device processes the media stream by using a pure software MTP, regardless of the nature of the stream, which enables video and data streams to be processed in addition to audio streams. When the pass-through mode is set in a transcoding profile, no transcoding is done for the session; the transcoding device performs a pure software MTP function. The pass-through mode can be used for secure Real-Time Transport Protocol (RTP) sessions.

Examples

The following example shows how to set the call density and codec complexity to g729abr8:

```
Router(config)# dspfarm profile 123 transcode
Router(config-dspfarm-profile)# codec g729abr8
```

The following example shows how to set up a video conference with guaranteed-audio.

```
Router(config)# dspfarm profile 99 conference video guaranteed-audio
Router(config-dspfarm-profile)# codec h264 4cif
Router(config-dspfarm-profile)# codec h264 cif
Router(config-dspfarm-profile)# maximum conference-participants 8
```

Related Commands

Command	Description
associate application	Associates the SCCP protocol to the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (DSP Farm profile)	Specifies the maximum number of sessions that are supported by the profile.
rsvp	Enables RSVP support on a transcoding or MTP device.
maximum conference-participants (DSP Farm profile)	Specifies the maximum number of conference participants that are supported by this profile.
shutdown (DSP Farm profile)	Disables a DSP farm profile.

codec (voice-card)

To specify call density and codec complexity according to the codec standard that is being used or to increase processing frequency for the G.711 codec, use the **codec** command in voice-card configuration mode. To reset the flex complexity default or to disable configured values, use the **no** form of this command.

codec {**complexity** {**flex** [**reservation-fixed** {**high** | **medium**}] | **high** | **medium** | **secure**} | **sub-sample**}

no codec complexity

Syntax Description

complexity	Manages the complexity and density of codecs used in voice processing.
flex	When the **flex** keyword is used, up to 16 calls can be completed per digital signal processor (DSP). The number of supported calls varies from 6 to 16, depending on the codec used for a call. In this mode, reservation for analog voice interface cards (VICs) may be needed for certain applications such as Central Automatic Message Accounting (CAMA) E-911 calls because oversubscription of DSPs is possible. If this is true, enable the **reservation-fixed** keyword. There is no reservation by default.
reservation-fixed	(Optional) If you have specified the **flex** keyword, the **reservation-fixed** keyword ensures that sufficient DSP resources are available to handle a call. If you enter the **reservation-fixed** keyword, set the complexity for **high** or **medium**. (See the guidelines following to understand the effects of the keywords.) This option appears only when there is an analog VIC present.
high	If you specify the **high** keyword to define the complexity, each DSP supports two voice channels encoded in any of the following formats: • g711alaw—G.711 a-law 64,000 bps. • g711ulaw—G.711 mu-law 64,000 bps. • g723ar53—G.723.1 Annex A 5300 bps. • g723ar63—G.723.1 Annex A 6300 bps. • g723r53—G.723.1 5300 bps. • g723r63—G.723.1 6300 bps. • g726r16—G.726 16,000 bps. • g726r24—G726 24,000 bps. • g726r32—G.726 32,000 bps. • g728—G.728 16,000 bps. • g729r8—G.729 8000 bps. This is the default. • g729br8—G.729 Annex B 8000 bps. • fax relay—2400 bps, 4800 bps, 7200 bps, 9600 bps, 12 kbps, and 14.4 kbps. **Note** Codecs G.723.1 and G.728 are not supported on Cisco 1750 and Cisco 1751 modular access routers for Cisco Hoot and Holler over IP applications.

medium	If you specify the **medium** keyword to define the complexity, each DSP supports four voice channels encoded in any of the following formats: • g711alaw—G.711 a-law 64,000 bps. • g711ulaw—G.711 mu-law 64,000 bps. • g726r16—G.726 16,000 bps. • g726r24—G.726 24,000 bps. • g726r32—G.726 32,000 bps. • g729r8—G.729 Annex A 8000 bps. • g729br8—G.729 Annex B with Annex A 8000 bps. • fax relay—2400 bps, 4800 bps, 7200 bps, 9600 bps, 12 kbps, and 14.4 kbps. Fax relay is the default.
secure	If you specify the **secure** keyword to define complexity, each DSP on an NM-HDV network module supports two voice channels encoded in any of the following formats: • g711alaw—G.711 a-law 64,000 bps. • g711ulaw—G.711 mu-law 64,000 bps. • g729—G.729 8000 bps. • g729A—G.729 8000 bps.
sub-sample	Increases the processing frequency for the G.711 codec with reduced 5510 DSP density.

Defaults

The default type of codec complexity is **flex**. The default value for the G.711 codec is 10 milliseconds (ms).

Command Modes

Voice-card configuration (config-voice-card)

Command History

Release	Modification
12.0(5)XK	This command was introduced as the codec complexity on the Cisco 2600 and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was implemented on the Cisco MC3810 for use with the high-performance compression module (HCM).
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1750 and Cisco 1751.
12.2(13)T	The **ecan-extended** keyword was added.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T with support for the Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745 routers. High codec complexity is supported for DSP processing on these platforms.

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ and the **flex** keyword was added. The **ecan-extended** keyword was removed and G.168 echo-cancellation compliance became the default.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T and the **reservation-fixed** keyword was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T and the **secure** keyword was added to provide secure codec complexity for TI-549 DSP processing on the NM-HDV network module.
12.4(22)T1	The **codec complexity** command was changed to the **codec** (voice-card) command and the **sub-sample** keyword was added for the 5510 DSP.

Usage Guidelines

Codec complexity refers to the amount of processing required to perform voice compression. Codec complexity affects the call density—the number of calls reconciled on the DSPs. With higher codec complexity, fewer calls can be handled. Select a higher codec complexity if that is required to support a particular codec or combination of codecs. Select a lower codec complexity to support the greatest number of voice channels, provided that the lower complexity is compatible with the particular codecs in use.

For codec complexity to change, all of the DSP voice channels must be in the idle state.

When you have specified the **flex** keyword, you can connect (or configure in the case of DS0 groups and PRI groups) more voice channels to the module than the DSPs can accommodate. If all voice channels should go active simultaneously, the DSPs become oversubscribed, and calls that are unable to allocate a DSP resource fail to connect. The **flex** keyword allows the DSP to process up to 16 channels. In addition to continuing support for configuring a fixed number of channels per DSP, the **flex** keyword enables the DSP to handle a flexible number of channels. The total number of supported channels varies from 6 to 16, depending on which codec is used for a call. Therefore, the channel density varies from 6 per DSP (high-complexity codec) to 16 per DSP (g.711 codec).

The **high** keyword selects a higher codec complexity if that is required to support a particular codec or combination of codecs. When you use the **codec complexity high** command to change codec complexity, the system prompts you to remove all existing DS0 or PRI groups using the specified voice card, then all DSPs are reset, loaded with the specified firmware image, and released.

The **medium** keyword selects a lower codec complexity to support the greatest number of voice channels, provided that the lower complexity is compatible with the particular codecs in use.

The **secure** keyword restricts the number of TI-549 DSP channels to 2, which is the lower codec complexity required to support Secure Real-Time Transport Protocol (SRTP) package capability on the NM-HDV and enable media authentication and encryption. If the **secure** command is not configured then the gateway will not advertise secure capability to Cisco CallManager, resulting in nonsecure calls. You do not need to use any command to specify secure codec complexity for TI-5510 DSPs, which support SRTP capability in all modes. Use the **mgcp package-capability** *srtp-package* command to enable MGCP gateway capability to process SRTP packages. Use the **show voice dsp** command to display codec complexity status.

Voice quality issues may occur when there are more than 15 G.711 channels on one 5510 DSP. To resolve the voice-quality issue, change the processing period (or segment size) of the G.711 codec from 5 ms to 10 ms. (The segment size of most voice codecs is 10 ms.) However, a voice call with 10-ms segment size has longer end-to-end delay (+ 5ms to 10 ms) than a call with 5-ms segment size.

Beginning in Cisco IOS Release 12.4(22)T1, the **sub-sample** keyword is added for applications that have strict requirements for round-trip delay times for VoIP. You can now accept the default G.711 (10 ms with lower MIPS) or enter the **codec sub-sample** command to select 5-ms G.711 (lower delay with higher MIPS). The **sub-sample** keyword is enabled only for the 5510 DSP.

The **codec sub-sample** command enables 5-ms processing for the G.711 codec inside the DSP to reduce the delay. However, this reduces the channel density of G.711 channels from 16 to 14. There is no difference in secure channel density when this mode is enabled.

Examples

The following example sets the codec complexity to high on voice card 1 installed on a router, and configures local calls to bypass the DSP:

```
voice-card 1
 codec complexity high
local-bypass
```

The following example sets the codec complexity to secure on voice card 1 installed on the NM-HDV, and configures it to support SRTP package processing, media authentication, and encryption:

```
voice-card 1
 codec complexity secure
```

The following example shows how to enable 5-ms processing for the G.711 codec inside the 5510 DSP:

```
voice-card 1
 codec sub-sample
```

Related Commands

Command	Description
ds0-group	Defines T1/E1 channels for compressed voice calls and the CAS method by which the router connects to the PBX or PSTN.
mgcp package-capability	Enables MGCP gateway capability to process SRTP packages.
show voice dsp	Displays the current status of all DSP voice channels.

codec aal2-profile

To set the codec profile for a digital signal processor (DSP) on a per-call basis, use the **codec aal2-profile** command in dial peer configuration mode. To restore the default codec profile, use the **no** form of this command.

codec aal2-profile {**itut** | **custom** | **atmf**} *profile-number codec*

no codec aal2-profile

Syntax Description

itut	The *profile-number* as an ITU-T type.
custom	The *profile-number* as a custom type.
atmf	The *profile-number* as an Asynchronous Transfer Mode Forum (ATMF) type.
profile-number	The available *profile-number* selections depend on the profile type. For ITU-T: • **1** = G.711 mu-law • **2** = G.711 mu-law with silence insertion descriptor (SID) • **7** = G.711 mu-law and G.729ar8 For ATMF: **9** = Broadband Loop Emulation Services (BLES) support for VoAAL2 For custom: • **100** = G.711 mu-law and G.726r32 • **110** = G.711 mu-law, G.726r32, and G.729ar8
codec	Enter one codec for the DSP. The possible *codec* entries depend on the *profile-number* value. The valid entries are as follows: • For ITU 1—**g711 mu-law** • For ITU 2—**g711 mu-law** • For ITU 7—**g711 mu-law** or **g729ar8** • For ATMF—**g711 mu-law** • For custom 100—**g711 mu-law** or **g726r32** • For custom 110—**g711 mu-law** or **g726r32** or **g729ar8** • For lossless compression—**llcc**

Command Default ITU-T profile 1 (G.711 mu-law)

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco IAD2420 series.
12.3(4)XD	The lossless compression codec (**llcc**) keyword was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command to configure the DSP to operate with a specified profile type and codecs.

You must enter the **session protocol aal2-trunk** command before configuring the codec ATM adaptation Layer 2 (AAL2) profile.

This command is used instead of the **codec (dial peer)** command for AAL2 trunk applications.

Examples

The following example sets the codec AAL2 profile type to ITU-T and configures a profile number of 7, enabling codec G.729ar8:

```
dial-peer voice 100 voatm
 session protocol aal2-trunk
 codec aal2-profile itut 7 g729ar8
```

The following example sets the codec AAL2 profile type to custom and configures a profile number of 100, enabling codec G.726r32:

```
dial-peer voice 200 voatm
 session protocol aal2-trunk
 codec aal2-profile custom 100 g726r32
```

Related Commands

Command	Description
session protocol (dial peer)	Establishes a session protocol for calls between the local and remote routers via the packet network.

codec gsmamr-nb

To specify the Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec for a dial peer, use the **codec gsmamr-nb** command in dial peer voice configuration mode. To disable the GSMAMR-NB codec, use the **no** form of this command.

codec gsmamr-nb [**packetization-period 20**] [**encap rfc3267**] [**frame-format** {**bandwidth-efficient** | **octet-aligned** [**crc** | **no-crc**]}] [**modes** *modes-value*]

no codec gsmamr-nb

Syntax Description

packetization-period 20	(Optional) Sets the packetization period at 20 ms.
encap rfc3267	(Optional) Sets the encapsulation value to comply with RFC 3267.
frame-format	(Optional) Specifies a frame format. Supported values are octet-aligned and bandwidth-efficient. The default is octet-aligned.
crc | **no-crc**	(Optional) CRC is applicable only for octet-aligned frame format. If you enter bandwidth-efficient frame format, the crc | no-crc options will not be available because they are inapplicable.
modes	(Optional) The eight speech-encoding modes (bit rates between 4.75 and 12.2 kbps) available in the GSMAMR-NB codec.
modes-value	(Optional) Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7).

Command Default

Packetization period is **20** ms.
Encapsulation is **rfc3267**.
Frame format is **octet-aligned**.
CRC is **no-crc**.
Modes value is **0-7**.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **codec gsmamr-nb** command configures the GSMAMR-NB codec and its parameters on the Cisco AS5350XM and Cisco AS5400XM platforms.

Examples

The following example sets the codec to **gsmamr-nb** and sets parameters:

```
Router(config-dial-peer)# codec gsmamr-nb packetization-period 20 encap rfc3267
frame-format octet-aligned crc
```

Related Commands

Command	Description
codec complexity	Specifies call density and codec complexity based on the codec used.
show dial peer voice	Displays the codec setting for dial peers.

codec ilbc

To specify the voice coder rate of speech for a dial peer using the internet Low Bandwidth Codec (iLBC), use the **codec ilbc** command in dial peer configuration mode. To reset the default value, use the **no** form of this command.

codec ilbc [**mode** *frame_size* [**bytes** *payload_size*]]

no codec ilbc [**mode** *frame_size* [**bytes** *payload_size*]]

Syntax Description

mode	(Optional) Specifies the iLBC operating frame mode that is encapsulated in each packet.
frame_size	(Optional) iLBC operating frame in milliseconds (ms). Valid entries are: • 20—20ms frames for 15.2kbps bit rate • 30—30ms frames for 13.33 kbps bit rate Default is 20.
bytes	(Optional) Specifies the number of bytes in the voice payload of each frame.
payload_size	(Optional) Number of bytes in the voice payload of each frame. Valid entries are: • For **mode 20**—38, 76, 114, 152, 190, 228. Default is 38. • For **mode 30**—50, 100, 150, 200. Default is 50.

Command Default

20ms frames with a 15.2kbps bit rate.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use this command to define a specific voice coder rate of speech and payload size for a VoIP dial peer using an iLBC codec.

If codec values for the dial peers of a connection do not match, the call fails.

You can change the payload of each VoIP frame by using the **bytes** keyword. However, increasing the payload size can add processing delay for each voice packet.

Examples

The following example shows how to configure the iLBC codec on an IP-to-IP Gateway:

```
dial-peer voice 1 voip
 rtp payload-type cisco-codec-ilbc 100
 codec ilbc mode 30 bytes 200
```

Related Commands

Command	Description
show dial peer voice	Displays the codec setting for dial peers.

codec preference

To specify a list of preferred codecs to use on a dial peer, use the **codec preference** command in voice-class configuration mode. To disable this functionality, use the **no** form of this command.

codec preference *value codec-type* [**mode** {**independent** | **adaptive**}] [**frame-size** {**20** | **30** | **60** | **fixed**] [**bit rate** *value*] [**bytes** *payload-size*] [**packetization-period 20**] [**encap rfc3267**] [**frame-format** {**bandwidth-efficient** | **octet-aligned** [**crc** | **no-crc**]}] [**modes** *modes-value*]

no codec preference *value codec-type*

Syntax Description

value	The order of preference; 1 is the most preferred and 14 is the least preferred.
codec-type	The codec preferred. Values are as follows: • **clear-channel**—Clear Channel 64,000 bps. • **g711alaw**—G.711 a-law 64,000 bps. • **g711ulaw**—G.711 mu-law 64,000 bps. • **g722r-64**—G.722-64 at 64,000 bps. • **g723ar53**—G.723.1 Annex-A 5300 bps. • **g723ar63**—G.723.1 Annex-A 6300 bps. • **g723r53**—G.723.1 5300 bps. • **g723r63**—G.723.1 6300 bps. • **g726r16**—G.726 16,000 bps • **g726r24**—G.726 24,000 bps • **g726r32**—G.726 32,000 bps. • **g728**—G.728 16,000 bps. • **g729abr8**—G.729 ANNEX-A and B 8000 bps. • **g729br8**—G.729 ANNEX-B 8000 bps. • **g729r8**—G.729 8000 bps. • **gsmamr-nb**—Enables GSMAMR-NB codec capability. • **gsmfr**—Global System for Mobile Communications Full Rate (GSMFR) 13,200 bps. **Note** The **gsmfr** keyword is configurable only on the Cisco AS5350 and AS5400 with MSAv6 digital signal processors (DSPs). • **ilbc**—internet Low Bitrate Codec (iLBC) at 13,330 bps or 15,200 bps. • **isac**—Cisco internet Speech Audio Codec (iSAC) codec. • **transparent**—Enables codec capabilities to be passed transparently between endpoints. **Note** The **transparent** keyword is not supported when the **call-start** command is configured.
mode	(Optional) For iLBC and iSAC codecs only. Specifies the iLBC or iSAC operating frame mode that is encapsulated in each packet.

independent	(Optional) For iSAC codec only. Specifies that the configuration mode variable bit rate (VBR) is independent (value 1).
adaptive	(Optional) For iSAC codec only. Specifies that the configuration mode VBR is adaptive (value 0).
frame-size	(Optional) For iLBC and iSAC codecs only. Specifies the operating frame in milliseconds (ms). Valid entries are: • **20**—20-ms frames (iLBC only) • **30**—30-ms frames (iLBC or iSAC) • **60**—60-ms frames (iLBC or iSAC) • **fixed**—This keyword is applicable only for adaptive mode.
bit rate *value*	(Optional) Configures the target bit rate in kilobits per second. The range is 10 to 32.
bytes	(Optional) Specifies that the size of the voice frame is in bytes.
payload-size	(Optional) Number of bytes that you specify as the voice payload of each frame. Values depend on the codec type and the packet voice protocol.
packetization-period 20	(Optional) Sets the packetization period at 20 ms. This keyword is applicable only to GSMAMR-NB codec support.
encap rfc3267	(Optional) Sets the encapsulation value to comply with RFC 3267. This keyword is applicable only to GSMAMR-NB codec support.
frame-format	(Optional) Specifies a frame format. Supported values are **octet-aligned** and **bandwidth-efficient**. The default is **octet-aligned**. This keyword is applicable only to GSMAMR-NB codec support.
crc | no-crc	(Optional) Cyclic Redundancy Check (CRC) is applicable only for octet-aligned frame format. If you enter bandwidth-efficient frame format, the **crc | no-crc** options are not available because they are inapplicable. This keyword is applicable only to GSMAMR-NB codec support.
modes *modes-values*	(Optional) Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7). This argument is applicable only to GSMAMR-NB codec support.

Command Default

If this command is not entered, no specific types of codecs are identified with preference.

If you enter the **gsmamr-nb** keyword, the default values are as follows:

Packetization period is 20 ms.
Encap is **rfc3267**.
Frame format is **octet-aligned**.
CRC is **no-crc**.
Modes value is **0-7**.

If you enter the **isac** keyword, the default values are as follows:

Mode is **independent**.
Target bit-rate is **32000 bps**.
Framesize is **30ms**.

Command Modes Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300.
12.0(7)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco Release IOS Release 12.1(2)T.
12.1(5)T	This command was modified. The **gsmefr** and **gsmfr** keywords were added.
12.2(13)T3	This command was modified.The **transparent** keyword was added.
12.4(4)XC	This command was extended to include GSMAMR-NB codec parameters on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(11)T	This command was modified. The **ilbc** and **mode** keywords were added.
12.4(11)XJ2	This command was modified. The **gsmefr** and **gsmfr** keywords were removed as configurable codec options for all platforms with the exception of the **gsmfr** codec on the Cisco AS5400 and AS5350 with MSAv6 dsps.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(15)XY	This command was modified. The **g722r-64** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was modified. The **isac** keyword was added as a codec type, and the **independent**, **adaptive**, **bit rate**, and **fixed** keywords were added as configurable parameters.

Usage Guidelines The routers at opposite ends of the WAN may have to negotiate the codec selection for the network dial peers. The **codec preference** command specifies the order of preference for selecting a negotiated codec for the connection. Table 14 describes the voice payload options and default values for the codecs and packet voice protocols.

Note The **transparent** keyword is not supported when the **call start** command is configured.

Table 14 Voice Payload-per-Frame Options and Defaults

Codec	Protocol	Voice Payload Options (in Bytes)	Default Voice Payload (in Bytes)
g711alaw **g711ulaw**	VoIP VoFR VoATM	80, 160 40 to 240 in multiples of 40 40 to 240 in multiples of 40	160 240 240
g722r-64	VoIP	80, 160, 240	160

Table 14 Voice Payload-per-Frame Options and Defaults (continued)

Codec	Protocol	Voice Payload Options (in Bytes)	Default Voice Payload (in Bytes)
g723ar53 **g723r53**	VoIP VoFR VoATM	20 to 220 in multiples of 20 20 to 240 in multiples of 20 20 to 240 in multiples of 20	20 20 20
g723ar63 **g723r63**	VoIP VoFR VoATM	24 to 216 in multiples of 24 24 to 240 in multiples of 24 24 to 240 in multiples of 24	24 24 24
g726r16	VoIP VoFR VoATM	20 to 220 in multiples of 20 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g726r24	VoIP VoFR VoATM	30 to 210 in multiples of 30 15 to 240 in multiples of 15 30 to 240 in multiples of 15	60 90 90
g726r32	VoIP VoFR VoATM	40 to 200 in multiples of 40 20 to 240 in multiples of 20 40 to 240 in multiples of 20	80 120 120
g728	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	40 60 60
g729abr8 **g729ar8** **g729br8** **g729r8**	VoIP VoFR VoATM	10 to 230 in multiples of 10 10 to 240 in multiples of 10 10 to 240 in multiples of 10	20 30 30
ilbc	VoIP	For the **mode 20** keyword, 38, 76, 114, 152, 190, 228 For the **mode 30** keyword, 50, 100, 150, 200	38 50
iSAC	VoIP	—	—

Examples

The following example show how to set the codec preference to the GSMAMR-NB codec and specify parameters:

```
Router(config-voice-class)# codec preference 1 gsmamr-nb packetization-period 20 encap
rfc3267 frame-format octet-aligned crc
```

The following example shows how to create codec preference list 99 and applies it to dial peer 1919:

```
voice class codec 99
codec preference 1 g711alaw
codec preference 2 g711ulaw bytes 80
codec preference 3 g723ar53
codec preference 4 g723ar63 bytes 144
codec preference 5 g723r53
codec preference 6 g723r63 bytes 120
codec preference 7 g726r16
codec preference 8 g726r24
codec preference 9 g726r32 bytes 80
codec preference 10 g729br8
codec preference 11 g729r8 bytes 50
end
```

```
dial-peer voice 1919 voip
 voice-class codec 99
```

The following example shows how to configure the transparent codec used by the Cisco Unified Border Element:

```
voice class codec 99
codec preference 1 transparent
```

Note You can assign a preference value of 1 only to the transparent codec. Additional codecs assigned to other preference values are ignored if the transparent codec is used.

The following example shows how to configure the iLBC codec used by the Cisco Unified Border Element:

```
voice class codec 99
codec preference 1 ilbc mode 30 bytes 200
```

Related Commands

Command	Description
call-start	Forces an H.323 Version 2 gateway to use fast connect or slow connect procedures for a dial peer.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number to a codec voice class.
voice-class codec (dial peer)	Assigns a previously configured codec selection preference list to a dial peer.

codec profile

To define video capabilities needed for video endpoints, use the **codec profile** command in telephony-service configuration mode. To disable the codec profile, use the **no** form of this command.

codec profile *tag profile*

no codec profile

Syntax Description

tag	A number in the range of 1 to 1000000.
profile	The name of the audio or video codec profile: • aacld • h263 • h263+ • h264

Command Default No codec profile is configured.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines For the Cisco Unified Customer Voice Portal solution, only h263 and h263+ are supported profile options.

Examples The following example shows the codec tagged 116 assigned to the H263 profile.

```
codec profile 116 H263
    clockrate 90000
    fmtp "fmtp:120 SQCIF=1;QCIF=1;CIF=1;CIF4=2;MAXBR=3840;I=1"
```

The codec profile can then be added to a voice class codec list, or the VoIP dial peer:

```
voice class codec 998
 codec preference 1 g711ulaw
 video codec h263 profile 116
```

Related Commands

Command	Description
clockrate	Sets the clock rate for the codec.
fmtp	Defines a string for video endpoints.

comfort-noise

To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated, use the **comfort-noise** command in voice-port configuration mode. To provide silence when the remote party is not speaking and VAD is enabled at the remote end of the connection, use the **no** form of this command.

comfort-noise

no comfort-noise

Syntax Description

This command has no arguments or keywords.

Command Default

Background noise is generated by default.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and was implemented on the Cisco 2600 series, the Cisco 7200 series, and the Cisco 7500 series using the extended echo canceller.

Usage Guidelines

Use the **comfort-noise** command to generate background noise to fill silent gaps during calls if VAD is activated. If the **comfort-noise** command is not enabled, and VAD is enabled at the remote end of the connection, the user hears dead silence when the remote party is not speaking.

The configuration of the **comfort-noise** command affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

Examples

The following example enables background noise on voice port 1/0/0:

```
voice-port 1/0/0
 comfort-noise
```

Related Commands

Command	Description
vad (dial peer configuration)	Enables VAD for the calls using a particular dial peer.
vad (voice-port configuration)	Enables VAD for the calls using a particular voice port.

compand-type

To specify the companding standard used to convert between analog and digital signals in pulse code modulation (PCM) systems, use the **compand-type** command in voice-port configuration mode. To disable the compand type, use the **no** form of this command.

compand-type {**u-law** | **a-law**}

no compand-type {**u-law** | **a-law**}

Syntax Description

u-law	Specifies the North American mu-law ITU-T PCM encoding standard.
a-law	Specifies the European a-law ITU-T PCM encoding standard.

Command Default

mu-law (T1 digital)
a-law (E1 digital)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced.

Usage Guidelines

The Cisco 2660 and the Cisco 3640 routers do not require configuration of the **compand-type a-law** command. However, if you request a list of commands, the **compand-type a-law** command displays.

Note On the Cisco 3600 series routers router, the mu-law and a-law settings are configured using the **codec** dial peer configuration command.

Note This command is not supported on the Cisco AS 5300/5350/5400 and 5850 Universal Gateway series which use the Nextport DSP.

Examples

The following example configures a-law encoding on voice port 1/1:

```
voice-port 1/1
 compand-type a-law
```

Related Commands

Command	Description
codec (voice-port configuration)	Configures voice compression.

conference

To define a Feature Access Code (FAC) to initiate a three-party conference in feature mode on analog phones connected to FXS ports, use the **conference** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

conference *keypad-character*

no conference

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0—9, *, #). Default is #3.

Command Default

The default value is #3.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for the Call Conference feature from the default (#3) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Examples

The following example shows how to change the value of the feature code for Call Conference from the default (#3). With this configuration, a phone user presses hook flash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, the user presses hook flash to get the feature tone and then dials 33 to initiate a three-party conference.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# conference 33
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

conference-join custom-cptone

To associate a custom call-progress tone to indicate joining a conference with a DSP farm profile, use the **conference-join custom-cptone** command in DSP farm profile configuration mode. To remove the custom call-progress tone association and disable the tone for the conference profile, use the **no** form of this command.

conference-join custom-cptone *cptone-name*

no conference-join custom-cptone *cptone-name*

Syntax Description

cptone-name	Descriptive identifier for this custom call-progress tone that indicates joining a conference.

Command Default

No custom call-progress tone to indicate joining a conference is associated with the DSP farm profile.

Command Modes

DSP farm profile configuration

Command History

Cisco IOS Release	Version	Modification
12.4(11)XJ2	Cisco Unified CME 4.1	This command was introduced.
12.4(15)T	Cisco Unified CME 4.1	This command was integrated into Cisco IOS Release 12.4(15)T

Usage Guidelines

To have a tone played when a party joins a conference, define the join tone, then associate it with the DSP farm profile for that conference.

- Use the **voice class custom-cptone** command to create a voice class for defining custom call-progress tones to indicate joining a conference.
- Use the **cadence** and **frequency** commands to define the characteristics of the join tone.
- Use the **conference-join custom-cptone** command to associate the join tone to the DSP farm profile for that conference. Use the **show dspfarm profile command** to display the DSP farm profile.

Examples

The following example defines a custom call-progress tone to indicate joining a conference and associates that join tone to a DSP farm profile defined for conferencing. Note that the custom call-progress tone names in the **voice class custom-cptone** and **conference-join custom-cptone** commands must be the same.

```
Router(config)# voice class custom-cptone jointone
Router(cfg-cptone)# dualtone conference
Router(cfg-cp-dualtone)# frequency 500 500
Router(cfg-cp-dualtone)# cadence 100 100 100 100 100
!
Router(config)# dspfarm profile 1 conference
Router(config-dspfarm-profile)# conference-join custom-cptone jointone
```

Related Commands

Command	Description
cadence	Defines the tone-on and tone-off durations for a call-progress tone.
conference-leave	Associates a custom call-progress tone to indicate leaving a conference with a DSP farm profile.
daultone conference	Enters cp-dualtone configuration mode for specifying a custom call-progress tone.
frequency	Defines the frequency components for a call-progress tone.
show dspfarm profile	Display configured digital signal processor (DSP) farm profile information.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones to be detected.

conference-leave custom-cptone

To associate a custom call-progress tone to indicate leaving a conference with a DSP farm profile, use the **conference-leave custom-cptone** command in DSP farm profile configuration mode. To remove the custom call-progress tone association and disable the tone for the conference profile, use the **no** form of this command.

conference-leave custom-cptone *cptone-name*

no conference-leave custom-cptone *cptone-name*

Syntax Description

cptone-name	Descriptive identifier for this custom call-progress tone that indicates leaving a conference.

Command Default

No custom call-progress tone to indicate leaving a conference is is associated with the DSP farm profile.

Command Modes

DSP farm profile configuration

Command History

Cisco IOS Release	Version	Modification
12.4(11)XJ2	Cisco Unified CME 4.1	This command was introduced.
12.4(15)T	Cisco Unified CME 4.1	This command was integrated into Cisco IOS Release 12.4(15)T

Usage Guidelines

For a tone to be played when a party leaves a conference, define the leave tone, then associate it with the DSP farm profile for that conference.

Use the **voice class custom-cptone** command to create a voice class for defining custom call-progress tones to indicate leaving a conference.

Use the **cadence** and **frequency** commands to define the characteristics of the leave tone.

Use the **conference-join custom-cptone** command to associate the leave tone to the DSP farm profile for that conference. Use the **show dspfarm profile command** to display the DSP farm profile.

Examples

The following example defines a custom call-progress tone to indicate leaving a conference and associates that leave tone to a DSP farm profile defined for conferencing. Note that the custom call-progress tone names in the **voice class custom-cptone** and **conference-join custom-cptone** commands must be the same.

```
Router(config)# voice class custom-cptone leavetone
Router(cfg-cptone)# dualtone conference
Router(cfg-cp-dualtone)# frequency 500 500
Router(cfg-cp-dualtone)# cadence 100 100 100 100 100
!
Router(config)# dspfarm profile 1 conference
Router(config-dspfarm-profile)# conference-join custom-cptone leavetone
```

Related Commands

Command	Description
cadence	Defines the tone-on and tone-off durations for a call-progress tone.
conference-join	Associates a custom call-progress tone to indicate joining a conference with a DSP farm profile.
dualtone conference	Enters cp-dualtone configuration mode for specifying a custom call-progress tone.
frequency	Defines the frequency components for a call-progress tone.
show dspfarm profile	Display configured digital signal processor (DSP) farm profile information.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones to be detected.

condition

To manipulate the signaling format bit-pattern for all voice signaling types, use the **condition** command in voice-port configuration mode. To turn off conditioning on the voice port, use the **no** form of this command.

condition {**tx-a-bit** | **tx-b-bit**| **tx-c-bit**| **tx-d-bit**} {**rx-a-bit** | **rx-b-bit**| **rx-c-bit**| **rx-d-bit**} {**on** | **off** | **invert**}

no condition {**tx-a-bit** | **tx-b-bit**| **tx-c-bit**| **tx-d-bit**} {**rx-a-bit** | **rx-b-bit**| **rx-c-bit**| **rx-d-bit**} {**on** | **off** | **invert**}

Syntax Description

tx-a-bit	Sends A bit.
tx-b-bit	Sends B bit.
tx-c-bit	Sends C bit.
tx-d-bit	Sends D bit.
rx-a-bit	Receives A bit.
rx-b-bit	Receives B bit.
rx-c-bit	Receives C bit.
rx-d-bit	Receives D bit.
on	Forces the bit state to 1.
off	Forces the bit state to 0.
invert	Inverts the bit state.

Command Default

The signaling format is not manipulated (for all sent or received A, B, C, and D bits).

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **condition** command to manipulate the sent or received bit patterns to match expected patterns on a connected device. Be careful not to destroy the information content of the bit pattern. For example, forcing the a-bit on or off prevents Foreign Exchange Office (FXO) interfaces from being able to generate both an on-hook and off-hook state.

The **condition** command is applicable to digital voice ports only.

Examples

The following example manipulates the signaling format bit pattern on digital voice port 0:5:

```
voice-port 0:5
 condition tx-a-bit invert
 condition rx-a-bit invert
```

The following example manipulates the signaling format bit pattern on voice port 1/0:0:

```
voice-port 1/0:0
 condition tx-a-bit invert
 condition rx-a-bit invert
```

Related Commands

Command	Description
define	Defines the transmit and receive bits for North American E&M and E&M MELCAS voice signaling.
ignore	Configures the North American E&M or E&M MELCAS voice port to ignore specific receive bits.

connect (channel bank)

To define connections between T1 or E1 controller ports for the channel bank feature, use the **connect** command in global configuration mode. To restore default values, use the **no** form of this command.

connect *connection-id* **voice-port** *voice-port-number* {**t1** | **e1**} *controller-number ds0-group-number*

no connect *connection-id* **voice-port** *voice-port-number* {**t1** | **e1**} *controller-number ds0-group-number*

Syntax Description

connection-id	A name for this connection.
voice-port	Specifies that a voice port is used in the connection.
voice-port-number	The voice port slot number and port number.
t1	Specifies a T1 port.
e1	Specifies an E1 port.
controller-number	The location of the first T1 or E1 controller to be connected. Valid values for the slot and port are 0 and 1.
ds0-group-number	The number identifier of the DS0 group associated with the first T1 or E1 controller port. The number is created by using the **ds0-group** command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

Command Default

There is no drop-and-insert connection between the ports.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.2(15)ZJ	The **voice-port** keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **connect** command creates a named connection between two DS0 groups associated with voice ports on T1 or E1 interfaces where the groups have been defined by the **ds0-group** command.

Examples

The following example shows how to configure a channel bank connection for FXS loop-start signaling:

```
Router(config)# controller t1 1/0
Router(config-controller)# ds0-group 1 timeslot 0 type fxo-loop-start
Router(config-controller)# exit
Router(config)# voice-port 1/1/0
Router(config-voiceport)# signal-type fxs-loop-start
Router(config-voiceport)# exit

Router(config)# connect connection1 voice-port 1/1/0 t1 1/0 0
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and the signaling type by which the router communicates with the PBX or PSTN.
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.

connect (drop-and-insert)

To define connections among T1 or E1 controller ports for drop-and-insert (also called TDM cross-connect), use the **connect** command in global configuration mode. To restore default values, use the **no** form of this command.

connect *connection-id* {**t1** | **e1**} *slot*/*port-1 tdm-group-no-1* {**t1** | **e1**} *slot*/*port-2 tdm-group-no-2*

no connect *connection-id* {**t1** | **e1**} *slot*/*port-1 tdm-group-no-1* {**t1** | **e1**} *slot*/*port-2 tdm-group-no-2*

Syntax Description

connection-id	A name for this connection.
t1	Specifies a T1 port.
e1	Specifies an E1 port.
slot/*port-1*	The location of the first T1 or E1 controller to be connected. Range for *slot* and *port* is 0 and 1.
tdm-group-no-1	The number identifier of the TDM) group associated with the first T1 or E1 controller port and created by using the **tdm-group** command. Range is from 0 to 23 for T1 and from 0 to 30 for E1.
slot/*port-2*	The location of the second T1 or E1 controller port to be connected. Range for *slot* is from 0 to 5, depending on the platform. Range for *port* is from 0 to 3, depending on the platform and the presence of a network module.
tdm-group-no-2	The number identifier of the TDM group associated with the second T1 or E1 controller and created by using the **tdm-group** command. Range is from 0 to 23 for T1 and from 0 to 30 for E1.

Command Default There is no drop-and-insert connection between the ports.

Command Modes Global configuration

Command History

Release	Modification
12.0(5)XK	The command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(1)T	The command was modified to accommodate two channel groups on a port for 1- and 2-port T1/E1 multiflex voice/WAN interface cards (VWICs) on the Cisco 3600 series.

Usage Guidelines The **connect** command creates a named connection between two TDM groups associated with drop-and-insert ports on T1 or E1 interfaces where you have already defined the groups by using the **tdm-group** command.

Once TDM groups are created on two different physical ports, use the **connect** command to start the passage of data between the ports. If a crosspoint switch is provided in the AIM slot, the connections can extend between ports on different cards. Otherwise, the connection is restricted to ports on the same VWIC.

The VWIC can make a connection only if the number of time slots at the source and destination are the same. For the connection to be error-free, the two ports must be driven by the same clock source; otherwise, slips occur.

Examples

The following example shows a fractional T1 terminated on port 0 using time slots 1 through 8, a fractional T1 is terminated on port 1 using time slots 2 through 12, and time slots 13 through 20 from port 0 are connected to time slots 14 through 21 on port 1 by using the **connect** command:

```
controller t1 0/0
 channel-group 1 timeslots 1-8
 tdm-group 1 timeslots 13-20
 exit
controller t1 0/1
 channel-group 1 timeslots 2-12
 tdm-group 2 timeslot 14-21
 exit
 connect exampleconnection t1 0/0 1 t1 0/1 2
```

Related Commands

Command	Description
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

connect atm

To define connections between T1 or E1 controller ports and the ATM interface, enter the **connect atm** command in global configuration mode. Use the **no** form of this command to restore the default values.

connect *connection-id* **atm** *slot/port-1 virtual-circuit-name* | *vpi/vci* {**atm** | **T1** | **E1**} *slot/port-2 TDM-group-number* | {*virtual-circuit-name* | *vpi/vci*}

no connect *connection-id* **atm** *slot/port-1 virtual-circuit-name* | *vpi/vci* {**atm** | **T1** | **E1**} *slot/port-2 TDM-group-number* | {*virtual-circuit-name* | *vpi/vci*}

Syntax Description

connection-id	A name for this connection.
atm	Specifies the first ATM interface.
slot/port-1	The location of the ATM controller to be connected.
virtual-circuit- name	Specifies the permanent virtual circuit (PVC) or switched virtual circuit (SVC).
vpi/vci	Specifies a virtual path identifier (VPI) and virtual channel identifier (VCI).
atm	Specifies the second ATM interface.
T1	Specifies a T1 port.
E1	Specifies an E1 port.
slot/port-2	The location of the T1 or E1 controller to be connected.
TDM-group-number	The number identifier of the time-division multiplexing (TDM) group associated with the T1 or E1 controller port and created by using the **tdm-group** command. Range is 0 to 23 for T1 and 0 to 30 for E1.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced for ATM interfaces on the Cisco 2600 series and Cisco 3600 series.
12.3(4)XD	ATM-to-ATM connections are allowed.
12.3(7)T	Support for ATM-to-ATM connections was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command is used on Cisco 2600, Cisco 3600, and Cisco 3700 series routers to provide connections between T1/E1 and ATM interfaces. This command is used after all interfaces are configured.

After TDM groups are created on two different physical ports, you can use the **connect atm** command to start the passage of data between the ports. If a crosspoint switch is provided in the advanced integration module (AIM) slot, the connections can extend between ports on different cards. Otherwise, the connection is restricted to ports on the same VWIC card.

The VWIC can make a connection only if the number of time slots at the source and destination are the same. For the connection to be error free, the two ports must be driven by the same clock source; otherwise, slips occur.

Examples

The following example shows how the ATM permanent virtual circuit (PVC) and T1 TDM group are set up and then connected:

```
interface atm 1/0
 pvc pvc1 10/100 ces
 exit
controller T1 1/1
 tdm-group 3 timeslots 13-24 type e&m
 exit
connect tdm1 atm 1/0 pvc1 10/100 T1 1/1 3
```

Related Commands

Command	Description
tdm-group	Creates TDM groups that can be connected.
pvc	Creates a private virtual circuit.

connect interval

To specify the amount of time that a given digital signal processor (DSP) farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect, use the **connect interval** command in SCCP Cisco Unified CallManager configuration mode. To reset to the default value, use the **no** form of this command.

connect interval *seconds*

no connect interval

Syntax Description

seconds	Timer value, in seconds. Range is 1 to 3600. Default is 60.

Command Default

60 seconds

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the connect interval value to meet your needs.

Examples

The following example specifies that the profile attempts to connect to another Cisco Unified CallManager after 1200 seconds (20 minutes) when the current Cisco Unified CallManager connection fails:

```
Router(config-sccp-ccm)# connect interval 1200
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified CallManager with a Cisco Unified CallManager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified CallManager group.
bind interface	Binds an interface to a Cisco Unified CallManager group.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager connections fails.
sccp ccm group	Creates a Cisco Unified CallManager group and enters SCCP Cisco Unified CallManager configuration mode.

connect retries

To specify the number of times that a digital signal processor (DSP) farm attempts to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager connections fails, use the **connect retries** command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

connect retries *number*

no connect retries

Syntax Description

number	Number of connection attempts. Range is 1 to 32. Default is 3.

Command Default

3 connection attempts

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The value of this command specifies the number of times that the given DSP farm attempts to connect to the higher-priority Cisco Unified CallManager before it gives up and attempts to connect to the next Cisco Unified CallManager.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the connect retries value to meet your needs.

Examples

The following example allows a DSP farm to make 5 attempts to connect to the Cisco Unified CallManager before giving up and attempting to connect to the next Cisco Unified CallManager specified in the group:

```
Router(config-sccp-ccm)# connect retries 5
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified CallManager with a Cisco CallManager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco CallManager group.
bind interface	Binds an interface to a Cisco CallManager group.

Command	Description
connect interval	Specifies how many times a given profile attempts to connect to the specific Cisco Unified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.

connection

To specify a connection mode for a voice port, use the **connection** command in voice-port configuration mode. To disable the selected connection mode, use the **no** form of this command.

connection {**plar** | **tie-line** | **plar opx** [**cut-through-wait** | **immediate**]} *phone-number* | {**trunk** *phone-number* [**answer-mode**]}

connection {**plar** | **tie-line** | **plar opx** [**cut-through-wait** | **immediate**]} *phone-number* | {**trunk** *phone-number* [**answer-mode**]}

Syntax Description

plar	Specifies a private line automatic ringdown (PLAR) connection. PLAR is an autodialing mechanism that permanently associates a voice interface with a far-end voice interface, allowing call completion to a specific telephone number or PBX without dialing. When the calling telephone goes off-hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX.
tie-line	Specifies a connection that emulates a temporary tie-line trunk to a private branch exchange (PBX). A tie-line connection is automatically set up for each call and torn down when the call ends.
plar opx	Specifies a PLAR off-premises extension (OPX) connection. Using this option, the local voice port provides a local response before the remote voice port receives an answer. On Foreign Exchange Office (FXO) interfaces, the voice port does not answer until the remote side has answered.
cut-through-wait	(Optional) Specifies that the router waits for the off-hook signal before cutting through the audio path. **Note** This keyword suppresses the subtle clicking sound that is heard when a phone goes off-hook. Users may have difficulty perceiving when the local FXO port has gone off-hook.
immediate	(Optional) Configures the FXO port to set up calls immediately (without waiting for Caller ID information) so the ring-cycle perception is identical for the caller and the called party. When the Caller ID is available, it is forwarded to the called number if the called party has not already answered the call. **Note** This option cannot be configured on an FXO port that is configured as a Centralized Automatic Message Accounting (CAMA) port.
phone-number	Specifies the destination telephone number. Valid entries are any series of digits that specify the E.164 telephone number.
trunk	Specifies a connection that emulates a permanent trunk connection to a PBX. A trunk connection remains permanent in the absence of any active calls.
answer-mode	(Optional) Specifies that the router does not initiate a trunk connection but waits for an incoming call before establishing the trunk. Use only with the **trunk** keyword.

Command Default

No connection mode is specified, and the standard session application outputs a dial tone when the interface goes off-hook until enough digits are collected to match a dial peer and complete the call.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA1	This command was implemented on the Cisco MC3810, and the **tie-line** keyword added.
11.3(1)MA5	The **plar opx** keyword was implemented on the Cisco MC3810 as the **plar-opx-ringrelay** keyword. The keyword was shortened in a subsequent release.
12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T.
12.0(3)XG	The **trunk** keyword was implemented on the Cisco MC3810. The **trunk answer-mode** option was added.
12.0(4)T	This command was integrated in Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was unified across the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.3(8)T	The **cut-through-wait** keyword was added.
12.4(11)XW	The **immediate** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

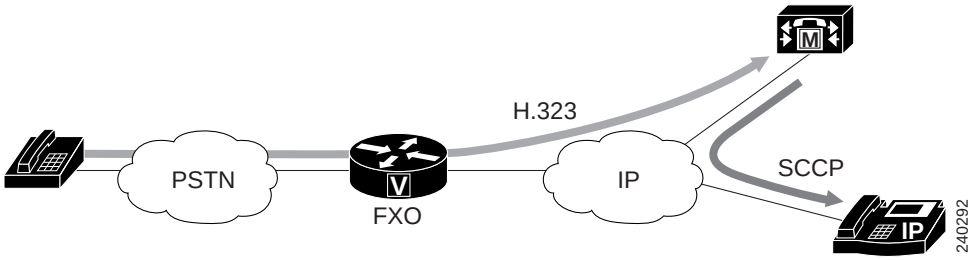
Usage Guidelines

Use the **connection** command to specify a connection mode for a specific interface. For example, use the **connection plar** command to specify a PLAR interface. The string you configure for this command is used as the called number for all incoming calls over this connection. The destination peer is determined by the called number.

The **connection plar opx immediate** option enables FXO ports to set up calls with no ring discrepancy for Caller ID between the caller and the called party. To implement the FXO Delayed Caller ID Delivery feature, you must have a configured network with a Cisco 2800 or Cisco 3800 series integrated services router running Cisco IOS Release 12.4(11)XW. The integrated services router must have at least one voice interface card. Cisco CallManager Release 4.2.3 SR1 or later releases must be installed on the network to support this feature.

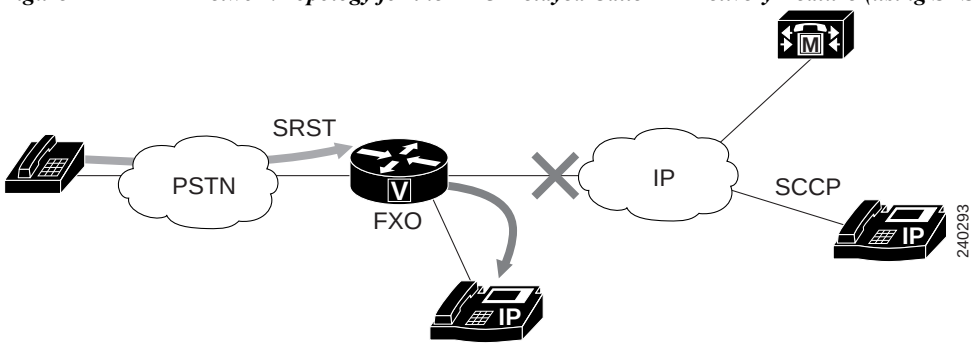
Figure 3 and Figure 4 show the network topology and call flow for the FXO Delayed Caller ID feature. The caller is in the PSTN, and the call arrives via an FXO port at the gateway. In Figure 3, the gateway is connected via H.323 to Cisco CallManager. Cisco CallManager extends the call to the called party which is a SCCP-based IP phone (Cisco 7941).

Figure 3 Network Topology for the FXO Delayed Caller ID Delivery Feature



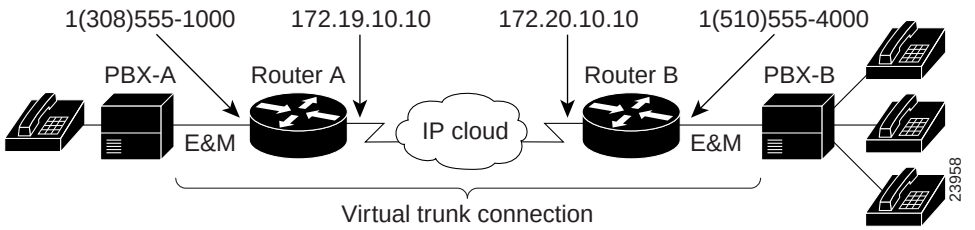
In Figure 4, the gateway is on the same router, and Survivable Remote Site Telephony (SRST) is active. SRST extends the call to the called party, which is a Skinny Client Control Protocol (SCCP)-based IP phone (Cisco 7941).

Figure 4 Network Topology for the FXO Delayed Caller ID Delivery Feature (using SRST)



Use the **connection trunk** command to specify a permanent tie-line connection to a PBX. VoIP simulates a trunk connection by creating virtual trunk tie lines between PBXs connected to Cisco devices on each side of a VoIP connection (see Figure 5). In this example, two PBXs are connected using a virtual trunk. PBX-A is connected to Router A via an E&M voice port; PBX-B is connected to Router B via an E&M voice port. The Cisco routers spoof the connected PBXs into believing that a permanent trunk tie line exists between them.

Figure 5 Virtual Trunk Connection



When configuring virtual trunk connections in VoIP, the following restrictions apply:

- You can use the following voice port combinations:
  - E&M to E&M (same type)
  - Foreign Exchange Station (FXS) to Foreign Exchange Office (FXO)
  - FXS to FXS (with no signaling)
- Do not perform number expansion on the destination pattern telephone numbers configured for trunk connection.
- Configure both end routers for trunk connections.

Note Because virtual trunk connections do not support number expansion, the destination patterns on each side of the trunk connection must match exactly.

To configure one of the devices in the trunk connection to act as slave and only receive calls, use the **answer-mode** option with the **connection trunk** command when configuring that device.

Note When using the **connection trunk** command, you must enter the **shutdown** command followed by the **no shutdown** command on the voice port.

VoIP establishes the trunk connection immediately after configuration. Both ports on either end of the connection are dedicated until you disable trunking for that connection. If for some reason the link between the two switching systems goes down, the virtual trunk reestablishes itself after the link comes back up.

Use the **connection tie-line** command when the dial plan requires you to add digits in front of any digits dialed by the PBX, and the combined set of digits is used to route the call onto the network. The operation is similar to the **connection plar** command operation, but in this case, the tie-line port waits to collect thedigits from the PBX. Tie-line digits are automatically stripped by a terminating port.

Examples

The following example shows PLAR as the connection mode with a destination telephone number of 555-0100:

```
voice-port 1/0/0
 connection trunk 5550100
```

The following example shows the tie-line as the connection mode with a destination telephone number of 555-0100:

```
voice-port 1/1
 connection tie-line 5550100
```

The following example shows a PLAR off-premises extension connection with a destination telephone number of 555-0100:

```
voice-port 1/0/0
 connection plar-opx 5550100
```

The following example shows a trunk connection configuration that is established only when the trunk receives an incoming call:

```
voice-port 1/0/0
 connection trunk 5550100 answer-mode
```

The following example shows a PLAR off-premises extension connection with a destination telephone number of 0199. The router waits for the off-hook signal before cutting through the audio path:

```
voice-port 2/0/0
 connection plar opx 0199 cut-through-wait
```

The following examples show configuration of the routers on both sides of a VoIP connection (as illustrated in Figure 5) to support trunk connections.

Router A

```
voice-port 1/0/0
 connection trunk +15105550190
dial-peer voice 10 pots
 destination-pattern +13085550181
 port 1/0/0
dial-peer voice 100 voip
 session-target ipv4:172.20.10.10
 destination-pattern +15105550190
```

Router B

```
voice-port 1/0/0
 connection trunk +13085550180
dial-peer voice 20 pots
 destination-pattern +15105550191
 port 1/0/0
dial-peer voice 200 voip
 session-target ipv4:172.19.10.10
 destination-pattern +13085550180
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix or the full E.164 telephone number for a dial peer.
dial peer voice	Enters dial peer configuration mode and specifies the voice encapsulation type.
session-protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session-target	Configures a network-specific address for a dial peer.
shutdown	Takes a specific voice port or voice interface card offline.
voice-port	Enters voice-port configuration mode.

connection-timeout

To configure the time in seconds for which a connection is maintained after completion of a communication exchange, use the **connection-timeout** command in settlement configuration mode. To return to the default value, use the **no** form of this command.

connection-timeout *seconds*

no connection-timeout *seconds*

Syntax Description

seconds	Time, in seconds, for which a connection is maintained after the communication exchange is completed. Range is from 0 to 86400; 0 means that the connection does not time out. The default is 3600 (1 hour).

Command Default

3600 seconds (1 hour)

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The router maintains the connection for the configured period in anticipation of future communication exchanges to the same server.

Examples

The following example shows a connection configured to be maintained for 3600 seconds after completion of a communications exchange:

```
settlement 0
 connection-timeout 3600
```

Related Commands

Command	Description
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up or shuts down the settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

copy flash vfc

To copy a new version of VCWare from the Cisco AS5300 universal access server motherboard to voice feature card (VFC) flash memory, use the **copy flash vfc** command in privileged EXEC mode.

copy flash vfc *slot-number*

Syntax Description

slot-number	Slot on the Cisco AS5300 in which the VFC is installed. Range is from 0 to 2.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3NA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **copy flash vfc** command to use the standard copy user interface in order to copy a new version of VCWare from the Cisco AS5300 universal access server motherboard to VFC flash memory. The VFC is a plug-in feature card for the Cisco AS5300 universal access server and has its own Flash memory storage for embedded firmware. For more information about VFCs, refer to *Voice-over-IP Card*.

Once the VCWare file has been copied, use the **unbundle vfc** command to uncompress and install VCWare.

Examples

The following example copies a new version of VCWare from the Cisco AS5300 universal access server motherboard to VFC flash memory:

```
Router# copy flash vfc 0
```

Related Commands

Command	Description
copy tftp vfc	Copies a new version of VCWare from a TFTP server to VFC flash memory.
unbundle vfc	Unbundles the current running image of VCWare or DSPWare into separate files.

copy tftp vfc

To copy a new version of VCWare from a TFTP server to voice feature card (VFC) flash memory, use the **copy tftp vfc** command in privileged EXEC mode.

copy tftp vfc *slot-number*

Syntax Description

slot-number	Slot on the Cisco AS5300 in which the VFC is installed. Range is from 0 to 2. There is no default.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3NA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **copy tftp vfc** command to copy a new version of VCWare from a TFTP server to VFC flash memory. The VFC is a plug-in feature card for the Cisco AS5300 universal access server and has its own flash storage for embedded firmware. For more information about VFCs, refer to *Voice-over-IP Card*.

Once the VCWare file has been copied, use the **unbundle vfc** command to uncompress and install VCWare.

Examples

The following example copies a file from the TFTP server to VFC flash memory:

```
Router# copy tftp vfc 0
```

Related Commands

Command	Description
copy flash vfc	Copies a new version of VCWare from the Cisco AS5300 motherboard to VFC flash memory.
unbundle vfc	Unbundles the current running image of VCWare or DSPWare into separate files.

corlist incoming

To specify the class of restrictions (COR) list to be used when a specified dial peer acts as the incoming dial peer, use the **corlist incoming** command in dial peer configuration mode. To clear the previously defined incoming COR list in preparation for redefining the incoming COR list, use the **no** form of this command.

corlist incoming *cor-list-name*

no corlist incoming *cor-list-name*

Syntax Description

cor-list-name	Name of the dial peer COR list that defines the capabilities that the specified dial peer has when it is used as an incoming dial peer.

Command Default No default behavior or values.

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines The **dial-peer cor list** and **member** commands define a set of capabilities (a COR list). These lists are used in dial peers to indicate the capability set that a dial peer has when it is used as an incoming dial peer (the **corlist incoming** command) or to indicate the capability set that is required for an incoming dial peer to make an outgoing call through the dial peer (the **corlist outgoing** command). For example, if dial peer 100 is the incoming dial peer and its incoming COR list name is list100, dial peer 200 has list200 as the outgoing COR list name. If list100 does not include all the members of list200 (that is, if list100 is not a superset of list200), it is not possible to have a call from dial peer 100 that uses dial peer 200 as the outgoing dial peer.

Examples In the following example, incoming calls from 526.... are blocked from being switched to outgoing calls to 1900.... because the COR list for the incoming dial peer (list2) is not a superset of the COR list for the outgoing dial peer (list1):

```
dial-peer list list1
 member 900call

dial-peer list list2
 member 800call
 member othercall

dial-peer voice 526 pots
 answer-address 408555....
 corlist incoming list2
 direct-inward-dial
```

```
dial-peer voice 900 pots
 destination pattern 1900.......
 direct-inward-dial
 trunkgroup 101
 prefix 333
 corlist outgoing list1
```

Related Commands

Command	Description
corlist outgoing	Specifies the COR list to be used by outgoing dial peers.
dial-peer cor list	Defines a COR list name.
member	Adds a member to a dial peer COR list.

corlist outgoing

To specify the class of restrictions (COR) list to be used by outgoing dial peers, use the **corlist outgoing** command in dial peer configuration mode. To clear the previously defined outgoing COR list in preparation for redefining the outgoing COR list, use the **no** form of this command.

corlist outgoing *cor-list-name*

no corlist outgoing *cor-list-name*

Syntax Description

cor-list-name	Required name of the dial peer COR list for outgoing calls to the configured number using this dial peer.

Command Default No default behavior or values.

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines If the COR list for the incoming dial peer is not a superset of the COR list for the outgoing dial peer, calls from the incoming dial peer cannot use that outgoing dial peer.

Examples In the following example, incoming calls from 526.... are blocked from being switched to outgoing calls to 1900.... because the COR list for the incoming dial peer (list2) is not a superset of the COR list for the outgoing dial peer (list1):

```
dial-peer list list1
member 900call

dial-peer list list2
 member 800call
 member othercall

dial-peer voice 526 pots
 answer-address 408555....
 corlist incoming list2
 direct-inward-dial

dial-peer voice 900 pots
 destination pattern 1900.......
 direct-inward-dial
 trunk group 101
 prefix 333
 corlist outgoing list1
```

cptone

To specify a regional analog voice-interface-related tone, ring, and cadence setting for a voice port, use the **cptone** command in voice-port configuration mode. To disable the selected tone, use the **no** form of this command.

cptone *locale*

no cptone *locale*

Syntax Description

locale	Country-specific voice-interface-related default tone, ring, and cadence setting (for ISDN PRI and E1 R2 signaling). Keywords are shown in Table 15. The default keyword is **us** in Cisco IOS Release 12.0(4)T and later releases.

Command Default

The default keyword is **us** for all supported gateways and interfaces in Cisco IOS Release 12.0(4)T and later releases.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was modified. The full keyword names for the countries were first added on the Cisco MC3810.
12.0(4)T	This command was modified. ISO 3166 two-letter country codes were added on the Cisco MC3810.
12.1(5)XM	This command was modified. The following keywords were added: **eg**, **gh**, **jo**, **ke**, **lb**, **ng, np**, **pa, pk**, **sa**, and **zw**.
12.2(2)T	This command was implemented on the Cisco 1750 and integrated into Cisco IOS Release 12.2(2)T.
12.2(15)ZJ	This command was modified. The **c1** and **c2** keywords were added for the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(15)T	This command was modified. The following keywords were added: **ae**, **kw**, and **om**.
15.0(1)M	This command was modified. The **cl** keyword was added.
15.1(3)T	This command was modified. The **mt** keyword was added.

Usage Guidelines

This command defines the detection of call-progress tones generated at the local interface. It does not affect any information passed to the remote end of a connection, and it does not define the detection of tones generated at the remote end of a connection. Use the **cptone** command to specify a regional analog voice interface-related default tone, ring, and cadence setting for a specified voice port.

If your device is configured to support E1 R2 signaling, the E1 R2 signaling type (whether ITU, ITU variant, or local variant as defined by the **cas-custom** command) must match the appropriate pulse code modulation (PCM) encoding type as defined by the **cptone** command. For countries for which a **cptone** value has not yet been defined, you can try the following:

- If the country uses a-law E1 R2 signaling, use the **gb** value for the **cptone** command.
- If the country uses mu-law E1 R2 signaling, use the **us** value for the **cptone** command.

Table 15 lists valid entries for the *locale* argument.

Table 15 Valid Command Entries for* locale *Argument

Country	cptone *locale* Command Entry	Country	cptone *locale* Command Entry
Argentina	**ar**	Lebanon	**lb**
Australia	**au**	Luxembourg	**lu**
Austria	**at**	Malaysia	**my**
Belgium	**be**	Malta	**mt**
Brazil	**br**	Mexico	**mx**
Canada	**ca**	Nepal	**np**
Chile	**cl**	Netherlands	**nl**
China	**cn**	New Zealand	**nz**
Colombia	**co**	Nigeria	**ng**
Custom 1[1]	**c1**	Norway	**no**
Custom 2[1]	**c2**	Oman	**om**
Czech Republic	**cz**	Pakistan	**pk**
Denmark	**dk**	Panama	**pa**
Egypt	**eg**	Peru	**pe**
Finland	**fi**	Philippines	**ph**
France	**fr**	Poland	**pl**
Germany	**de**	Portugal	**pt**
Ghana	**gh**	Russian Federation	**ru**
Great Britain	**gb**	Saudi Arabia	**sa**
Greece	**gr**	Singapore	**sg**
Hong Kong	**hk**	Slovakia	**sk**
Hungary	**hu**	Slovenia	**si**
Iceland	**is**	South Africa	**za**
India	**in**	Spain	**es**

Table 15 Valid Command Entries for **locale** *Argument (continued)*

Country	cptone *locale* Command Entry	Country	cptone *locale* Command Entry
Indonesia	**id**	Sweden	**se**
Ireland	**ie**	Switzerland	**ch**
Israel	**il**	Taiwan	**tw**
Italy	**it**	Thailand	**th**
Japan	**jp**	Turkey	**tr**
Jordan	**jo**	United Arab Emirates	**ae**
Kenya	**ke**	United States	**us**
Korea Republic	**kr**	Venezuela	**ve**
Kuwait	**kw**	Zimbabwe	**zw**

1. Automatically configured the first time the XML file is downloaded to the gateway.

Examples

The following example configures United States as the call-progress tone locale:

```
voice-port 1/0/0
 cptone us
```

The following example configures Brazil as the call-progress tone locale on a Cisco universal access server:

```
voice-port 1:0
 cptone br
 description Brasil Tone
```

Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.
cas-custom	Customizes signaling parameters for a particular E1 or T1 channel group on a channelized line.

cptone call-waiting repetition interval

To set the call-waiting alert pattern on analog endpoints that are connected to Foreign Exchange Station (FXS) ports, use the **cptone call-waiting repetition interval** command in supplementary-service voice-port configuration mode. To return to the default behavior, use the **no** form of this command.

cptone call-waiting repetition interval *second*

no cptone call-waiting repetition interval

Syntax Description

second	Length of time, in seconds for the tone repetition interval. Range: 0 to 30. Default: 0.

Command Default

A single-beep tone is the default behavior.

Command Modes

Supplementary-service voice-port configuration (config-stcapp-suppl-serv-port)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **cptone call-waiting repetition interval** command to set the call-waiting alert pattern on analog endpoints that are connected to FXS ports on a Cisco IOS voice gateway, such as a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway.

When configured, the ringtone periodically repeats with configured interval until either the user switches to the new call or the calling party hangs up.

Examples

The following example shows how to set the call-waiting alert pattern on analog endpoints connected to port 2/0 on a Cisco VG224:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# cptone call-waiting repetition interval 20
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

credential load

To reload a credential file into flash memory, use the **credential load** command in privileged EXEC mode.

credential load *tag*

Syntax Description

tag	Number that identifies the credential (.csv) file to load. Range: 1 to 5. This is the number that was defined with the **authenticate credential** command.

Command Default The credential file is not reloaded.

Command Modes Privileged EXEC

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines This command provides a shortcut to reload credential files that were defined with the **authenticate credential** command.

Up to five .csv files can be configured and loaded into the system. The contents of these five files are mutually exclusive, that is, the username/password pairs must be unique across all the files. For Cisco Unified CME, these username/password pairs cannot be the same ones defined for SCCP or SIP phones with the **username** command.

Examples The following example shows how to reload credential file 3:

```
credential load 3
```

Related Commands

Command	Description
authenticate (voice register global)	Defines the authenticate mode for SIP phones in a Cisco Unified CME or Cisco Unified SRST system.
username (ephone)	Defines a username and password for SCCP phones.
username (voice register pool)	Defines a username and password for authenticating SIP phones.

credentials (SIP UA)

To configure a Cisco IOS Session Initiation Protocol (SIP) time-division multiplexing (TDM) gateway, a Cisco Unified Border Element (Cisco UBE), or Cisco Unified Communications Manager Express (Cisco Unified CME) to send a SIP registration message when in the UP state, use the **credentials** command in SIP UA configuration mode. To disable SIP digest credentials, use the **no** form of this command.

credentials {**dhcp** | **number** *number* **username** *username*} **password** [**0** | **7**] *password* **realm** *realm*

no credentials {**dhcp** | **number** *number* **username** *username*} **password** [**0** | **7**] *password* **realm** *realm*

Syntax Description

dhcp	(Optional) Specifies the Dynamic Host Configuration Protocol (DHCP) is to be used to send the SIP message.
number *number*	(Optional) A string representing the registrar with which the SIP trunk will register (must be at least four characters).
username *username*	A string representing the username for the user who is providing authentication (must be at least four characters). This option is only valid when configuring a specific registrar using the **number** keyword.
password	Specifies password settings for authentication.
0	(Optional) Specifies the encryption type as cleartext (no encryption). This is the default.
7	(Optional) Specifies the encryption type as encrypted.
password	A string representing the password for authentication. If no encryption type is specified, the password will be cleartext format. The string must be between 4 and 128 characters.
realm *realm*	(Optional) A string representing the domain where the credentials are applicable.

Command Default

SIP digest credentials are disabled.

Command Modes

SIP UA configuration (sip-ua)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
12.4(22)YB	This command was modified. The **dhcp** keyword was added and the **username** keyword and *username* argument were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. The **number** keyword and *number* argument were added and the **username** keyword and *username* argument reintroduced to configure credentials for a given registrar when multiple registrars are configured.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

The following configuration rules are applicable when credentials are enabled:

- Only one password is valid for all domain names. A new configured password overwrites any previously configured password.
- The password will always be displayed in encrypted format when the **credentials** command is configured and the **show running-config** command is used.

The **dhcp** keyword in the command signifies that the primary number is obtained via DHCP and the Cisco IOS SIP TDM gateway, Cisco UBE, or Cisco Unified CME on which the command is enabled uses this number to register or unregister the received primary number.

Examples

The following example shows how to configure SIP digest credentials without specifying the password encryption type:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# credentials dhcp password MyPassword realm example.com
```

The following example shows how to configure SIP digest credentials using the encrypted format:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# credentials dhcp password 7 095FB01AA000401 realm example.com
```

The following example shows how to disable SIP digest credentials where the encryption type was specified:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# no credentials dhcp password 7 095FB01AA000401 realm example.com
```

The following example shows how to configure SIP digest credentials for two different realms without specifying the encryption type:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# credentials number 1111 username MyUser password MyPassword realm
MyLocation1.example.com
Router(config-sip-ua)# credentials number 1111 username MyUser password MyPassword realm
MyLocation2.example.com
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
registrar	Enables Cisco IOS SIP TDM gateways to register E.164 numbers for FXS, EFXS, and SCCP phones on an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

Cisco IOS Voice Commands: D

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order beginning with the letter D. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

default (auto-config application)

To configure an auto-config application configuration command to its default value, use the **default** command in auto-config application configuration mode.

default *command*

Syntax Description

command	One of the auto-config application configuration commands. Valid choices are as follows: • **retries** • **server** • **shutdown** • **timeout**

Command Default No default behavior or values

Command Modes Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples The following example shows the **default** command used to set the number of download retry attempts for an auto-configuration application to its default value.

```
Router(auto-config-app)# default retries
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
show auto-config	Displays the current status of auto-config applications.

default (MGCP profile)

To configure a Media Gateway Control Protocol (MGCP profile) command to its default value, use the **default** command in MGCP profile configuration mode. To disable the default command, use the **no** form of the command for that profile parameter.

default *command*

no default *command*

Syntax Description

command	One of the MGCP profile commands. Valid choices are as follows: • call-agent • description (MGCP profile) • max1 lookup • max1 retries • max2 lookup • max2 retries • package persistent • timeout tcrit • timeout tdinit • timeout tdmax • timeout tdmin • timeout thist • timeout tone busy • timeout tone cot1 • timeout tone cot2 • timeout tone dial • timeout tone dial stutter • timeout tone mwi • timeout tone network congestion • timeout tone reorder • timeout tone ringback • timeout tone ringback connection • timeout tone ringing • timeout tone ringing distinctive • timeout tpar • timeout tsmax • voice-port (MGCP profile)

Command Default No default behaviors or values

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for an MGCP profile.

The **default (MGCP profile)** command instructs the MGCP profile to use the default value of the specified command whenever the profile is called. This has the same effect as using the **no** form of the specified command, but the **default** command clearly specifies which commands are using their default values.

To use the default values for more than one command, enter each command on a separate line.

Examples The following example shows how to configure the default values for three MGCP profile commands:

```
Router(config)# mgcp profile newyork
Router(config-mgcp-profile)# default max1 retries
Router(config-mgcp-profile)# default timeout tdinit
Router(config-mgcp-profile)# default timeout tone mwi
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

default (SIP)

To reset a SIP command to its default value, use the **default** command in SIP configuration mode.

default *command*

Syntax Description

command	One of the SIP configuration commands. Valid choices are: • **bind**: Configures the source address of signaling and media packets to a specific interface's IP address. • **rel1xx**: Enables all SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint. • **session-transport**: Configures the underlying transport layer protocol for SIP messages to TCP or UDP. • **url**: Configures URLs to either the SIP or TEL format for your voip sip calls.

Defaults

The default is that binding is disabled (**no bind**).

Command Modes

SIP configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows how to reset the value of the SIP **bind** command:

```
Router(config)# voice serv voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# default bind
```

Related Commands

Command	Description
sip	Enter SIP configuration mode from voice-service VoIP configuration mode.

default-file vfc

To specify an additional (or different) file from the ones in the default file list and stored in voice feature card (VFC) Flash memory, use the **default-file vfc** command in global configuration mode. To delete the file from the default file list, use the **no** form of this command.

default-file *filename* **vfc** *slot*

no default-file *filename* **vfc** *slot*

Syntax Description

filename	Indicates the file to be retrieved from VFC Flash memory and used to boot up the system.
slot	Indicates the slot on the Cisco AS5300 in which the VFC is installed. Range is to 2. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for that version of VCWare. The default file list includes the files that is used to boot up the system.

Use the **default-file vfc** command to add a specified file to the default file list, replacing the existing default for that extension type.

Examples

The following example specifies that the bas-vfc-1.0.14.0.bin file, which is stored in VFC Flash memory, be added to the default file list:

```
default-file bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
cap-list vfc	Adds a voice codec overlay file to the capability file list.
delete vfc	Deletes a file from VFC Flash memory.

define

To define the transmit and receive bits for North American ear and mouth (E&M), E&M Mercury Exchange Limited Channel-Associated Signaling (MELCAS), and Land Mobile Radio (LMR) voice signaling, use the **define** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

define {**tx-bits** | **rx-bits**} {**seize** | **idle**} {**0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111**}

no define {**tx-bits** | **rx-bits**} {**seize** | **idle**} {**0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111**}

Syntax Description

tx-bits	The bit pattern applies to the transmit signaling bits.
rx-bits	The bit pattern applies to the receive signaling bits.
seize	The bit pattern defines the seized state.
idle	The bit pattern defines the idle state.
0000 through **1111**	Specifies the bit pattern.

Command Default

The default is to use the preset signaling patterns as defined in American National Standards Institute (ANSI) and European Conference of Postal and Telecommunications Administrations (CEPT) standards, as follows:

- For North American E&M:
  - tx-bits idle 0000 (0001 if on E1 trunk)
  - tx-bits seize 1111
  - rx-bits idle 0000
  - rx-bits seize 1111
- For E&M MELCAS:
  - tx-bits idle 1101
  - tx-bits seize 0101
  - rx-bits idle 1101
  - rx-bits seize 0101
- For LMR:
  - tx-bits idle 0000
  - tx-bits seize 1111
  - rx-bits idle 0000
  - rx-bits seize 1111

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA3	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	The command was integrated into Cisco IOS Release 12.1(2)T.
12.3(4)XD	The LMR signaling type was added to the signaling types to which this command applies.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

The **define** command applies to E&M digital voice ports associated with T1/E1 controllers.

Use the **define** command to match the E&M bit patterns with the attached telephony device. Be careful not to define invalid configurations, such as all 0000 on E1, or identical seized and idle states. Use this command with the **ignore** command.

In LMR signaling, the **define** command is used to define polarity on E&M analog and digital voice ports.

Examples

To configure a voice port on a Cisco 2600 or Cisco 3600 series router that is sending traffic in North American E&M signaling format to convert the signaling to MELCAS format, enter the following commands:

```
voice-port 1/0/0
 define rx-bits idle 1101
 define rx-bits seize 0101
 define tx-bits idle 1101
 define tx-bits seize 0101
```

In this example, reverse polarity is configured on a voice port on a Cisco 3700 series router that is sending traffic in LMR signaling format:

```
voice-port 1/0/0
 define rx-bits idle 1111
 define rx-bits seize 0000
 define tx-bits idle 1111
 define tx-bits seize 0000
```

Related Commands

Command	Description
condition	Manipulates the signaling bit-pattern for all voice signaling types.
ignore	Configures a North American E&M or E&M MELCAS voice port to ignore specific receive bits.

delete vfc

To delete a file from voice feature card (VFC) Flash memory, use the **delete vfc** command in privileged EXEC mode.

delete *filename* **vfc** *slot*

Syntax Description

filename	Specifies the file in VFC Flash memory to be deleted.
slot	Specifies the slot on the Cisco AS5300 in which the specified VFC resides. Range is from 0 to 2.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **delete vfc** command to delete a specific file from VFC Flash memory and to remove the file from the default list or capability list if the specified file is included in those lists.

Note Deleting a file from VFC Flash memory does not free the VFC Flash memory space that the file occupied. To free VFC Flash memory space, use the **erase vfc** command.

Examples

The following example deletes the bas-vfc-1.0.14.0.bin file, which is stored in VFC Flash memory of the VFC located in slot 0:

```
Router# delete bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
default-file vfc	Specifies an additional (or different) file from the ones in the default file list and stored in VFC Flash memory.
erase vfc	Erases the Flash memory of a specified VFC.
show vfc directory	Displays the list of all files that reside on this VFC.

description

To specify a description of the digital signal processor (DSP) interface, use the **description** command in voice-port or DSP farm interface configuration mode. To describe a MGCP profile that is being defined, use the **description** command in MGCP profile configuration mode. To specify the name or a brief description of a charging profile, use the **description** command in charging profile configuration mode. To delete a configured description, use the **no** form of the command in the appropriate configuration mode.

description *string*

no description

Syntax Description

string	Character string from 1 to 80 characters for DSP interfaces and MGCP profiles, or from 1 to 99 characters for charging profiles.

Command Default

Enabled with a null string.
The MGCP profile has no default description.
Charging profiles have no default description.

Command Modes

Voice-port configuration
DSP farm interface configuration
MGCP profile configuration
Charging profile configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series and Cisco 7200.
11.3(1)MA	This command in voice-port configuration mode was implemented on the Cisco MC3810.
12.0(5)XE	This command in DSP farm interface configuration mode was modified.
12.1(1)T	The DSP farm interface configuration mode modification was integrated into Cisco IOS Release 12.1(1)T.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2(11)T	Support for the Cisco AS5300 and Cisco AS5850 was added.
12.3(8)XU	This command was introduced in charging profile configuration mode.
12.3(11)YJ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(14)YQ.
12.4(9)T	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use the **description** command to describe the DSP interface connection or a defined MGCP profile. The information is displayed when a **show** command is used, and it does not affect the operation of the interface in any way.

Examples

The following example identifies voice port 1/0/0 as being connected to the purchasing department:

```
voice-port 1/0/0
 description purchasing_dept
```

The following example identifies DSP farm interface 1/0 as being connected to the marketing department:

```
dspint dspfarm 1/0
 description marketing_dept
```

The following example shows a description for an MGCP profile:

```
mgcp profile newyork
 description This is the head sales office in New York.
 dot ...(socket=0)
 S:.
 R:250 NAA09092 Message accepted for delivery
 S:QUIT
 R:221 madeup@abc.com closing connection
 Freeing SMTP ctx at 0x6121D454
 returned from work_routine, context freed
```

Related Commands

Command	Description
category	Identifies the subscriber category to which a charging profile applies.
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies, as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies, as a trigger condition in a charging profile, that the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies, as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
gprs charging characteristics reject	Specifies that create PDP context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	
gprs charging profile	Creates a new charging profile (or modifies an existing one) and enters charging profile configuration mode.

Command	Description
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of GGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

description (dial peer)

To add a description to a dial peer, use the **description** command in dial peer configuration mode. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Text string up to 64 alphanumeric characters.

Command Default Disabled

Command Modes Dial peer configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines Use this command to include descriptive text about the dial peer. The description displays in **show** command output and does not affect the operation of the dial peer.

Examples The following example shows a description included in a dial peer:

```
dial-peer voice 1 pots
 description inbound PSTN calls
```

Related Commands

Command	Description
dial-peer voice	Defines a dial peer.
show dial-peer voice	Displays configuration information for dial peers.

description (DSP Farm profile)

To include a description about the digital signal processor (DSP) farm profile, use the **description** command in DSP farm profile configuration mode. To remove a description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Character string from 1 to 80 characters.

Command Default No default behavior or values

Command Modes DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines Use this command to include descriptive text about this DSP farm profile. This information displays in **show** commands and does not affect the operation of the interface.

Examples The following example identifies the DSP farm profile as being designated to the art department:

```
Router(config-dspfarm-profile)# description art_dept
```

Related Commands

Command	Description
codec (DSP Farm profile)	Specifies the codecs supported by a DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (DSP Farm profile)	Specifies the maximum number of sessions that need to be supported by the profile.
shutdown (DSP Farm profile)	Allocates DSP farm resources and associates with the application.

description (dspfarm)

To include a specific description about the digital signal processor (DSP) interface, use the **description** command in DSPfarm interface configuration mode. To disable this feature, use the **no** form of this command.

description *string*

no description *string*

Syntax Description

string	Character string from 1 to 80 characters.

Command Default Enabled with a null string.

Command Modes DSPfarm interface configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for the Cisco 7200 series routers.
12.0(5)XE	This command was modified to reduce the maximum number of allowable characters in a text string from 255 to 80.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines Use the **description** command to include descriptive text about this DSP interface connection. This information is displayed when you issue a **show** command and does not affect the operation of the interface in any way.

Examples The following example identifies DSPfarm interface 1/0 on the Cisco 7200 series routers router as being connected to the marketing department:

```
dspint dspfarm 1/0
description marketing_dept
```

description (SCCP Cisco CallManager)

To include a description about the Cisco CallManager group, use the **description** command in SCCP Cisco CallManager configuration mode. To remove a description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Character string from 1 to 80 characters.

Command Default No default behavior or values

Command Modes SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines Use this command to include descriptive text about a Cisco CallManager group. This information is displayed in **show** commands and does not affect the operation of the interface.

Examples The following example identifies SCCP as being designated to the Boston office:

```
Router(config-sccp-ccm)# description boston office
```

Related Commands

Command	Description
associate ccm	Associates a Cisco CallManager with a Cisco CallManager group and establishes its priority within the group.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco CallManager when the current Cisco CallManager connections fails.
sccp ccm group	Creates a Cisco CallManager group and enters SCCP Cisco CallManager configuration mode.

description (trunk group)

To add a description to a trunk group, use the **description** command in trunk group configuration mode. To delete the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	Trunk group description. Maximum length is 63 alphanumeric characters.

Command Default No default behavior or values

Command Modes Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples The following example shows a description for a trunk group:

```
Router(config)# trunk group alpha1
Router(config-trunk-group)# description carrierAgroup1
```

Related Commands

Command	Description
trunk group	Initiates the definition of a trunk group.

description (voice source group)

To add a description to a voice source group, use the **description** command in voice source-group configuration mode. To delete the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	Describes a voice source group, Maximum length of the voice source group description is 63 alphanumeric characters.

Command Default No default behavior or values

Command Modes Voice source-group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples The following example shows a description for a voice source group:

```
Router(config)# voice source-group northern1
Router(cfg-source-grp)# description carrierBgroup3
```

Related Commands

Command	Description
voice source-group	Defines a source group for voice calls.

destination uri

To specify the voice class used to match a dial peer to the destination uniform resource identifier (URI) of an outgoing call, use the **destination uri** command in dial peer configuration mode. To remove the URI voice class, use the **no** form of this command.

destination uri *tag*

no destination uri

Syntax Description

tag	Alphanumeric label that uniquely identifies the voice class. This tag must be configured with the **voice class uri** command.

Command Default

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Before you use this command, configure the voice class by using the **voice class uri** command.
- This command applies new rules for dial-peer matching. Table 16 shows the rules and the order in which they are applied when the **destination uri** command is used. The gateway compares the dial-peer command to the call parameter in its search to match an outbound call to a dial peer. All dial peers are searched based on the first match criteria. Only if no match is found does the gateway move on to the next criteria.

Table 16 Dial-Peer Matching Rules for Outbound URI

Match Order	Cisco IOS Command	Outgoing Call Parameter
1	**destination uri** and **carrier-id target**	Application-provided URI and target carrier ID associated with the call
2	**destination-pattern** and **carrier-id target**	Called number and target carrier ID associated with the call
3	**destination uri**	Application-provided URI
4	**destination-pattern**	Called number
5	**carrier-id target**	Target carrier ID associated with the call

Note Calls whose destination is an E.164 number, rather than a URI, use the previously existing dial-peer matching rules. For information, see the *Dial Peer Configuration on Voice Gateway Routers* document, Cisco IOS Voice Library.

Examples

The following example matches the destination URI in the outgoing call by using voice class ab100:

```
dial-peer voice 100 voip
 destination uri ab100
```

Related Commands

Command	Description
answer-address	Specifies calling number to match for a dial peer.
debug voice uri	Displays debugging messages related to URI voice classes.
destination-pattern	Specifies telephone number to match for a dial peer.
dial-peer voice	Enters dial peer configuration mode to create or modify a dial peer.
incoming uri	Specifies the voice class that a VoIP dial peer uses to match the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
session protocol	Specifies a session protocol for calls between local and remote routers using the packet network.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

destination-pattern

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode. To disable the configured prefix or telephone number, use the **no** form of this command.

destination-pattern [**+**]*string*[**T**]

no destination-pattern [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used preceding a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default The command is enabled with a null string.

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.1(1)	The command was integrated into Cisco IOS Release 12.1(1).
12.0(7)XR	This command was implemented on the Cisco AS5300 and modified to support the plus sign, percent sign, question mark, brackets, and parentheses symbols in the dial string.
12.0(7)XK	This command was modified. Support for the plus sign, percent sign, question mark, brackets, and parentheses in the dial string was added to the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented on the Cisco 1750, Cisco 7200 series, and Cisco 7500 series. The modifications for the Cisco MC3810 in Cisco IOS Release12.0(7)XK are not supported in this release.
12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK for the Cisco MC3810 were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, the Cisco ICS7750, and the Cisco VG200.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

The pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers that correspond to the destination pattern. If you have configured a prefix, the prefix is prepended to the remaining numbers, creating a dial string that the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

There are areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **destination-pattern** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

Note Cisco IOS software does not verify the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example shows configuration of the E.164 telephone number 555-0179 for a dial peer:

```
dial-peer voice 10 pots
 destination-pattern +5550179
```

The following example shows configuration of a destination pattern in which the pattern “43” is repeated multiple times preceding the digits “555”:

```
dial-peer voice 1 voip
 destination-pattern 555(43)+
```

The following example shows configuration of a destination pattern in which the preceding digit pattern is repeated multiple times:

```
dial-peer voice 2 voip
 destination-pattern 555%
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550109 and 5550199:

```
dial-peer voice 3 vofr
 destination-pattern 55501[0-9]9
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550439, 5553439, 5555439, 5557439, and 5559439:

```
dial-peer voice 4 voatm
 destination-pattern 555[03579]439
```

The following example shows configuration of a destination pattern in which the digit-by-digit matching is prevented and the entire string is received:

```
dial-peer voice 2 voip
 destination-pattern 555T
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
dial-peer terminator	Designates a special character to be used as a terminator for variable-length dialed numbers.
incoming called-number (dial peer)	Specifies a digit string that can be matched by an incoming call to associate that call with a dial peer.
prefix	Specifies the prefix of the dialed digits for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

destination-pattern (interface)

To specify the ISDN directory number for the telephone interface, use the **destination-pattern** command in interface configuration mode. To disable the specified ISDN directory number, use the **no** form of this command.

destination-pattern *isdn*

no destination-pattern

Syntax Description

isdn	Local ISDN directory number assigned by your telephone service provider.

Command Default

A default ISDN directory number is not defined for this interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command is applicable to the Cisco 800 series routers.

You must specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco 800 Series Routers Software Configuration Guide*.

Do not specify an area code with the local ISDN directory number.

Examples

The following example specifies 555-0101 as the local ISDN directory number:

```
destination-pattern 5550101
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call-waiting	Disables call waiting.
port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show dial-peer voice	Displays configuration information and call statistics for dial peers.

detect v54 channel-group

To enable V.54 loopback detection for the command sent from the remote device, use the **detect v54 channel-group command in** controller configuration mode. To disable the V.54 loopback detection, use the **no** form of this command.

detect v54 channel-group *channel-number*

no detect v54 channel-group *channel-number*

Syntax Description

channel-number	Channel number from 1 to 24 (T1) or from 1 to 31 (E1).

Command Default

V.54 loopback detection is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Use the **detect v54 channel-group** controller configuration command to enable V.54 loopback detection. The remote device sends a loopup inband payload command sequence in fractional T1 (FT1).

Examples

The following example sets the loopback detection for channel-group 1; then the loopback detection is disabled for channel-group 1.

```
detect v54 channel-group 1
no detect v54 channel-group 1
```

Related Commands

Command	Description
loopback remote v54 channel-group	Activates a remote V.54 loopback for the channel group on the far end.

device-id

To identify a gateway associated with a settlement provider, use the **device-id** command in settlement configuration mode. To reset to the default value, use the **no** form of this command.

device-id *number*

no device-id *number*

Syntax Description

number	Device ID number as provided by the settlement server. Range is from 0 to 2147483647.

Command Default The default device ID is 0

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines It is optional to identify a gateway associated with a settlement provider.

Examples The following example sets the device ID to 1000:

```
settlement 0
 device-id 1000
```

Related Commands

Command	Description
customer-id	Identifies a carrier or Internet service provider with the settlement provider.
settlement	Enters settlement configuration mode.

dhcp interface

To configure an interface type for Dynamic Host Configuration Protocol (DHCP) provisioning of Session Initiation Protocol (SIP) parameters, use the **dhcp interface** command in SIP user-agent configuration mode.

dhcp interface *type number*

Syntax Description

type	Type of interface to be configured.
number	Port, connector, or interface card number. **Note** The number format varies depending on the network module or line card type and the router's chassis slot it is installed in. The numbers are assigned at the factory at the time of installation or when they are added to a system; they can be displayed with the **show interfaces** command.

Command Default

No interface type is configured for DHCP provisioning of SIP parameters.

Command Modes

SIP user-agent configuration (sip-ua)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

Multiple interfaces on the Cisco Unified Border Element can be configured with DHCP. The **dhcp interface** command specifies which one is the DHCP interface used with SIP.

This command does not have a **no** form.

Table 17 displays the keywords that represent the types of interfaces that can be configured with the **dhcp interface** command. Replace the *type* argument with the appropriate keyword from the table.

Table 17 Interface Type Keywords

Keyword	Interface Type
ethernet	Ethernet IEEE 802.3 interface.
fastethernet	100-Mbps Ethernet interface. In RITE configuration mode, specifies the outgoing (monitored) interface for exported IP traffic.
gigabitethernet	1000-Mbps Ethernet interface.
tengigabitethernet	10-Gigabit Ethernet interface.

Examples

The following example configures the Gigabit Ethernet interface of slot 0 port 0 as the DHCP interface for DHCP provisioning of SIP parameters:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ip address dhcp
Router(config-if)# sip-ua
Router(sip-ua)# dhcp interface gigabitethernet 0/0
```

Related Commands

Command	Description
show interfaces	Displays information about interfaces.
sip-ua	Enters SIP user-agent configuration mode.

dial-control-mib

To specify attributes for the call history table, use the **dial-control-mib** command in global configuration mode. To restore the default maximum size or retention time of the call history table, use the **no** form of this command.

dial-control-mib {**max-size** *number* | **retain-timer** *number*}

no dial-control-mib {**max-size** *number* | **retain-timer** *number*}

Syntax Description

max-size *number*	Specifies the maximum size of the call history table. Range is from 0 to 1200 table entries. **Note** Specifying a value of 0 prevents any further entries from being added to the table. Any existing table entries will be preserved for the duration specified with the **retain-timer** keyword.
retain-timer *number*	Specifies the duration, in minutes, for entries to remain in the call history table. Range is from 0 to 35791. **Note** Specifying a value of 0 prevents any further table entries from being retained, but does not affect any timer currently in effect. Therefore, any existing table entries will remain for the duration previously specified with the **retain-timer** keyword.

Command Default

The default call history table length is 50 table entries. The default retain timer is 15 minutes.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.0(1)XA	This command was first applied to the CDR feature on the Cisco MC3810.
12.0(2)T	The command was integrated into Cisco IOS Release 12.0(2)T.
12.3T	The maximum value for the *number* argument following the **max-size** keyword was increased to 1200 entries.
12.3(8)T	The maximum value of the *number* argument following the **retain-timer** keyword was decreased to 35791 minutes.

Examples

The following example configures the call history table to hold 400 entries, with each entry remaining in the table for 10 minutes:

```
dial-control-mib max-size 400
dial-control-mib retain-timer 10
```

dial-peer cor custom

To specify that named class of restrictions (COR) apply to dial peers, use the **dial-peer cor custom** command in global configuration mode.

dial-peer cor custom

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or keywords.

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines You must use the **dial-peer cor custom** command and the **name** command to define the names of capabilities before you can specify COR rules and apply them to specific dial peers.

Examples of possible names might include the following: call1900, call527, call9, and call911.

Note You can define a maximum of 64 COR names.

Examples The following example defines two COR names:

```
dial-peer cor custom
 name 900blackhole
 name CatchAll
```

Related Commands

Command	Description
name (dial peer cor custom)	Provides a name for a custom COR.

dial-peer cor list

To define a class of restrictions (COR) list name, use the **dial-peer cor list** command in global configuration mode. To remove a previously defined COR list name, use the **no** form of this command.

dial-peer cor list *list-name*

no dial-peer cor list *list-name*

Syntax Description

list-name	List name that is applied to incoming or outgoing calls to specific numbers or exchanges.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

A COR list defines a capability set that is used in the COR checking between incoming and outgoing dial peers.

Examples

The following example adds two members to the COR list named list1:

```
dial-peer cor list list1
 member 900block
 member 800_call
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named COR apply to dial peers.
member (dial peer cor list)	Adds a member to a dial peer COR list.
name (dial peer cor custom)	Provides a name for a custom COR.

dial-peer data

To create a data dial peer and to enter dial-peer configuration mode, use the **dial-peer data** command in global configuration mode. To remove a data dial peer, use the **no** form of this command.

dial-peer data *tag* **pots**

no dial-peer data *tag*

Syntax Description

tag	Specifies the dial-peer identifying number. Range is from 1 to 2147483647.
pots	Specifies an incoming POTS dial peer.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines A data dial peer should be defined only for incoming data calls. The **incoming called-number** and **shutdown** commands on the data dial peer are allowed. However, the following POTS dial-peer commands are disabled on a data dial peer:

- **answer-address**
- **carrier-id**
- **destination-pattern**
- **information-type**
- **port**
- **trunk-group-label**

Examples The following example is a data dial peer configuration:

```
dial-peer data 100 pots
 incoming called-number 100
```

The following example is a voice dial peer configuration:

```
dial-peer voice 2001 pots
 destination-pattern 2001
 no digit-strip
 port 3/1:1
```

Related Commands

Command	Description
dial-peer search	Optimizes voice or data dial-peer searches.
incoming called-number	Specifies an incoming called number of an MMoIP or POTS dial peer.
shutdown (dial peer)	Changes the administrative state of a selected dial peer from up to down.

dial-peer hunt

To specify a hunt selection order for dial peers, use the **dial-peer hunt command in** global configuration mode. To restore the default selection order, use the **no** form of this command.

dial-peer hunt *hunt-order-number*

no dial-peer hunt

Syntax Description

hunt-order-number	A number from 0 to 7 that selects a predefined hunting selection order: 0—Longest match in phone number, explicit preference, random selection. This is the default hunt order number. 1—Longest match in phone number, explicit preference, least recent use. 2—Explicit preference, longest match in phone number, random selection. 3—Explicit preference, longest match in phone number, least recent use. 4—Least recent use, longest match in phone number, explicit preference. 5—Least recent use, explicit preference, longest match in phone number. 6—Random selection. 7—Least recent use.

Command Default

The default is the longest match in the phone number, explicit preference, random selection (hunt order number 0).

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco MC3810, and Cisco AS5300.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **dial-peer hunt** dial peer configuration command if you have configured hunt groups. “Longest match in phone number” refers to the destination pattern that matches the greatest number of the dialed digits. “Explicit preference” refers to the **preference** setting in the dial peer configuration. “Least recent use” refers to the destination pattern that has waited the longest since being selected. “Random selection” weights all of the destination patterns equally in a random selection mode.

This command applies to POTS, VoIP, Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Multimedia Mail over Internet Protocol (MMOIP) dial peers.

Examples

The following example configures the dial peers to hunt in the following order: (1) longest match in phone number, (2) explicit preference, (3) random selection.

```
dial-peer hunt 0
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
preference	Specifies the preferred selection order of a dial peer within a hunt group.
show dial-peer voice	Displays configuration information for dial peers.

dial-peer inbound selection sip-trunk

To enable incoming SIP line-side calls to use the same dial-peer matching rules as SIP trunk-side calls, use the **dial-peer inbound selection sip-trunk** command in global configuration mode. To revert to the default behavior, use the **no** form of this command.

dial-peer inbound selection sip-trunk

no dial-peer inbound selection sip-trunk

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (SIP line-side and SIP trunk-side calls use different dial-peer matching rules).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T2	This command was introduced.

Usage Guidelines

This command applies the same dial-peer matching rules used for calls from SIP trunks to incoming calls from SIP phones (line side). Table 18 shows the rules and the order in which they are applied by default to SIP line-side calls. Table 19 shows the rules and the order in which they are applied to SIP trunk-side calls and to SIP line-side calls when the **dial-peer inbound selection sip-trunk** command is used.

The router compares the dial-peer configuration to the call parameter in its search to match an inbound call to a dial peer. All dial peers are searched based on the first match criteria. The router moves on to the next criteria only if no match is found.

Table 18 Dial-Peer Matching Rules for Inbound Calls from SIP Phones (Line Side)

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**destination-pattern**	Calling number
2	**answer-address**	Calling number
3	**incoming called-number**	Called number
4	**incoming uri request**	Request-URI
5	**incoming uri to**	To URI
6	**incoming uri from**	From URI
7	**carrier-id source**	Carrier-is associated with the call

Table 19 Dial-Peer Matching Rules for Inbound Calls from SIP Trunks

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri request**	Request-URI
2	**incoming uri to**	To URI
3	**incoming uri from**	From URI
4	**incoming called-number**	Called number
5	**answer-address**	Calling number
6	**destination-pattern**	Calling number
7	**carrier-id source**	Carrier-is associated with the call

Examples

The following example shows SIP line-side calls use the same matching rules as trunk-side calls:

```
dial-peer inbound selection sip-trunk
```

Related Commands

Command	Description
answer-address	Specifies calling number to match for a dial peer.
destination-pattern	Specifies telephone number to match for a dial peer.
dial-peer voice	Defines a specific dial peer.
incoming called-number	Incoming called number matched to a dial peer.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the uniform resource identifier (URI) of an incoming call.
show dial-peer voice	Displays configuration information for voice dial peers.

dial-peer no-match disconnect-cause

To disconnect the incoming ISDN or channel associated signaling (CAS) call when no inbound voice or modem dial peer is matched, use the **dial-peer no-match disconnect-cause** command in global configuration mode. To restore the default incoming call state (call is forwarded to the dialer), use the **no** form of this command.

dial-peer no-match disconnect-cause *cause-code-number*

no dial-peer no-match disconnect-cause *cause-code-number*

Syntax Description

cause-code-number	An ISDN cause code number. Range is from 1 to 127.

Command Default

The call is forwarded to the dialer to handle as a modem call.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

By default, calls are forwarded to the dialer to handle as a modem call when no inbound dial peer is matched. The **dial-peer no-match disconnect-cause** command changes that behavior to disconnect the incoming ISDN or CAS calls when no inbound voice or modem dial peer is matched.

Refer to the ISDN Cause Values table in the *Cisco IOS Debug Command Reference*, for a list of ISDN cause codes.

Examples

The following example shows that ISDN cause code 47 has been specified to match inbound voice or modem dial peers:

```
dial-peer no-match disconnect-cause 47
```

Related Commands

Command	Description
show dial-peer voice	Displays configuration information for dial peers.

dial-peer outbound status-check pots

To check the status of outbound POTS dial peers during call setup and to disallow, for that call, any whose status is down, use the **dial-peer outbound status-check pots** command in privileged EXEC mode. To disable status checking, use the **no** form of this command.

dial-peer outbound status-check pots

no dial-peer outbound status-check pots

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines Use this command to disallow, during call setup, outbound POTS dial peers (except those for e-phones) whose endpoints (voice ports or trunk groups) are down.

When the **dial-peer outbound status-check pots** command is configured, if the voice-port configured under an outbound POTS dial-peer is down, that dial-peer is excluded while matching the corresponding destination-pattern. Therefore, if there are no other matching outbound POTS dial-peers for the specified destination-pattern, the gateway will disconnect the call with a cause code of 1 (Unallocated/unassigned number), which is mapped to the "404 Not Found" SIP response by default. When the **no** form of this command is configured, the outbound POTS dial-peer is matched even if the voice-port configured under is down and the gateway disconnects the call with a cause code of 34 (No circuit/channel available), which is mapped to the "503 Service Unavailable" SIP response by default.

Note "503 Service Unavailable" was the default behavior before the **dial-peer outbound status-check pots** command was introduced. Users who need the original behavior should configure the **no** form of this command.

Table 20 shows conditions under which an outbound POTS dial peer may be up or down.

Table 20 Conditions Under Which an Outbound POTS Dial Peer Is Up or Down

If a Dial Peer's,,,	And If...	Then the Dial Peer Is...
Operational state is up	Its voice port is up	Up
	Its trunk groups and any associated trunks are up	
Operational state is down	—	Down
Voice port is down		
Trunk groups are down	All associated trunks are down	

To show or verify the status (up or down) of all or selected dial peers, use the **show dial-peer voice** command.

Examples

The following examples of output for the related **show dial-peer voice** command show the status of all or selected dial peers. You can use the **dial-peer outbound status-check pots** command to disallow the outbound POTS dial peers that are down.

The following example shows a short summary status for all dial peers. Outbound status is displayed in the OUT STAT field. POTS dial peers 31 and 42 are shown as down.

```
Router# show dial-peer voice summary

dial-peer hunt 0
              AD                                      PRE PASS                OUT
TAG    TYPE   MIN  OPER PREFIX    DEST-PATTERN       FER THRU SESS-TARGET    STAT PORT
444    voip   up   up                                 0
22     voip   up   up                                 0   syst
12     pots   up   up             5550123 0                        up   4/0:15
311    voip   up   up                                 0   syst
31     pots   up   up             5550111            0                       down 4/1:15
421    voip   up   up             5550199 0  syst ipv4:1.8.56.2
42     pots   up   up                                 0                       down
```

The following example shows the status for dial peer 12. Outbound status is displayed in the Outbound state field. The dial peer is shown as up.

```
Router# show dial-peer voice 12

VoiceEncapPeer12
        peer type = voice, information type = voice,
        description = `',
        tag = 12, destination-pattern = `5550123',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 12, Admin state is up, Operation state is up,
        Outbound state is up,                                  <------- display status
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        .
        .
        .
```

The following example shows the status for dial peer 31. Outbound status is displayed in the Outbound state field. The dial peer is listed as down.

```
Router# show dial-peer voice 31

VoiceEncapPeer31
        peer type = voice, information type = voice,
        description = `',
        tag = 31, destination-pattern = `5550111',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 31, Admin state is up, Operation state is up,
        Outbound state is down,                          <--------- display status
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        .
        .
        .
```

For descriptions of other significant fields shown in these outputs, see the **show dial-peer voice** command.

Related Commands

Command	Description
show dial-peer voice	Displays information for voice dial peers.

dial-peer search type

To optimize voice or data dial-peer searches, use the **dial-peer search type** command in global configuration mode. To disable the search parameters, use the **no** form of this command.

dial-peer search *type* {**data voice** | **voice data** | **none**}

no dial-peer search *type*

Syntax Description

data	Searches for data dial peers.
none	Searches for all dial peers by order of input.
voice	Searches for voice dial peers.

Command Default **data** and **voice**

Command Modes Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines The search defines the search preference explicitly. If the **data** and **voice** keywords are specified, data dial peers are searched first. If no data dial peers are found, the voice dial peers are searched.

Examples The following is sample output that shows that data dial peers are searched first. Then voice dial peers are searched if no data dial peers can be matched for an incoming call:

```
dial-peer search type data voice
```

The following is sample output that shows that voice dial peers are searched first. Then data dial peers are searched if no voice dial peers can be matched for an incoming call:

```
dial-peer search type voice data
```

Related Commands

Command	Description
dial-peer data	Enable a gateway to process incoming data calls first by assigning the POTS dial peer as data.

dial-peer terminator

To change the character used as a terminator for variable-length dialed numbers, use the **dial-peer terminator command in** global configuration mode. To restore the default terminating character, use the **no** form of this command.

dial-peer terminator *character*

no dial-peer terminator

Syntax Description

character	Designates the terminating character for a variable-length dialed number. Valid numbers and characters are #, *, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, and d. The default is #.

Command Default

The default terminating character is #

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0(7)XK	Usage was restricted to variable-length dialed numbers. The command was implemented on the Cisco 2600 series and Cisco 3600 series, and Cisco MC3810.
12.1(2)T	The command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

There are certain areas in the world (for example, in certain European countries) where telephone numbers can vary in length. When a dialed-number string has been identified as a variable length dialed-number, the system does not place a call until the configured value for the **timeouts interdigits** command has expired or until the caller dials the terminating character. Use the **dial-peer terminator** global configuration command to change the terminating character.

Examples

The following example shows that “9” has been specified as the terminating character for variable-length dialed numbers:

```
dial-peer terminator 9
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
show dial-peer voice	Displays configuration information for dial peers.

dial-peer video

To define a video ATM dial peer for a local or remote video codec, to specify video-related encapsulation, and to enter dial peer configuration mode use the **dial-peer video** command in global configuration mode. To remove the video dial peer, use the **no** form of this command.

dial-peer video *tag* {**videocodec** | **videoatm**}

no dial-peer video *tag* {**videocodec** | **videoatm**}

Syntax Description

tag	Digits that define a particular dial peer. Defines the dial peer and assigns the protocol type to the peer. Range is from 1 to 10000. The tag must be unique on the router.
videocodec	Specifies a local video codec connected to the router.
videoatm	Specifies a remote video codec on the ATM network.

Command Default

No video dial peer is configured

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The *tag* value must be unique to the device.

Examples

The following example sets up a local video dial peer designated as 10:

```
dial-peer video 10 videocodec
```

Related Commands

Command	Description
show dial-peer video	Displays dial peer video configuration.

dial-peer voice

To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial peer configuration mode, use the **dial-peer voice** command in global configuration mode. To delete a defined dial peer, use the **no** form of this command.

Cisco 1750 and Cisco 1751 Modular Access Routers

dial-peer voice *tag* {**pots** | **vofr** | **voip**}

no dial-peer voice *tag* {**pots** | **vofr** | **voip**}

Cisco 2600 Series, Cisco 2600XM, Cisco 3600 Series, and Cisco 3700 Series

dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip**}

no dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip**}

Cisco 7200 Series

dial-peer voice *tag* **vofr**

no dial-peer voice *tag* **vofr**

Cisco 7204VXR and Cisco 7206VXR

dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip**}

no dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip**}

Cisco AS5300

dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip**}

no dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip**}

Syntax Description

tag	Digits that define a particular dial peer. Range is from 1 to 2147483647.
pots	Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
vofr	Specifies that this is a Voice over Frame Relay (VoFR) dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network.
voip	Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
voatm	Specifies that this is a Voice over ATM (VoATM) dial peer that uses real-time ATM adaptation layer 5 (AAL5) voice encapsulation on the ATM backbone network.
mmoip	Indicates that this is a multimedia mail peer that uses IP encapsulation on the IP backbone.

Command Default

No dial peer is defined.
No method of voice encapsulation is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810, with support for the **pots**, **voatm**, **vofr**, and **vohdlc** keywords.
12.0(3)T	This command was implemented on the Cisco AS5300, with support for the **pots** and **voip** keywords.
12.0(3)XG	The **vofr** keyword was added for the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	The **vofr** keyword was added to the Cisco 7200 series.
12.0(4)XJ	The **mmoip** keyword was added for the Cisco AS5300. The **dial-peer voice** command was implemented for store-and-forward fax.
12.0(7)XK	The **voip** keyword was added for the Cisco MC3810, and the **voatm** keyword was added for the Cisco 3600 series. Support for the **vohdlc** keyword on the Cisco MC3810 was removed.
12.1(1)	The **mmoip** keyword addition in Cisco IOS Release 12.0(4)XJ was integrated into Cisco IOS Release 12.1(1). The **dial-peer voice** implementation for store-and-forward fax was integrated into this mainline release.
12.1(2)T	The keyword changes in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.1(5)T	This command was implemented on the Cisco AS5300 and integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command was implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the **dial-peer voice** global configuration command to switch to dial peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit** command to exit dial peer configuration mode and return to global configuration mode.

After you have created a dial peer, that dial peer remains defined and active until you delete it. To delete a dial peer, use the **no** form of this command. To disable a dial peer, use the **no shutdown** command in dial peer configuration mode.

In store-and-forward fax on the Cisco AS5300, the POTS dial peer defines the inbound faxing line characteristics from the sending fax device to the receiving Cisco AS5300 and the outbound line characteristics from the sending Cisco AS5300 to the receiving fax device. The Multimedia Mail over Internet Protocol (MMoIP) dial peer defines the inbound faxing line characteristics from the Cisco AS5300 to the receiving Simple Mail Transfer Protocol (SMTP) mail server. This command works with both on-ramp and off-ramp store-and-forward fax functions.

Note On the Cisco AS5300, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.

Examples

The following example shows how to access dial peer configuration mode and configure a POTS peer identified as dial peer 10 and an MMoIP dial peer identified as dial peer 20:

```
dial-peer voice 10 pots
dial-peer voice 20 mmoip
```

The following example deletes the MMoIP peer identified as dial peer 20:

```
no dial-peer voice 20 mmoip
```

The following example shows how the **dial-peer voice** command is used to configure the extended echo canceller. In this instance, **pots** indicates that this is a POTS peer using VoIP encapsulation on the IP backbone, and it uses the unique numeric identifier tag 133001.

```
Router(config)# dial-peer voice 133001 pots
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP for VoFR applications.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
shutdown	Changes the administrative state of the selected dial peer from up to down.

dial-type

To specify the type of out-dialing for voice port interfaces, use the **dial-type** command in voice-port configuration mode. To disable the selected type of dialing, use the **no** form of this command.

dial-type {**dtmf** | **pulse** | **mf**}

no dial-type

Syntax Description

dtmf	Dual tone multifrequency (DTMF) touch-tone dialing.
pulse	Pulse (rotary) dialing.
mf	Multifrequency tone dialing.

Command Default DTMF touch-tone dialing

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA3	This command was implemented on the Cisco MC3810, and the **pulse** keyword was added.
12.0(7)XK	The **mf** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was extended to the merged SGCP/MGCP software image.
12.2(2)T	This command was implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines Use the **dial-type** command to specify an out-dialing type for a Foreign Exchange Office (FXO) or E&M voice port interface. This command specifies the tone type for digit detection and out-pulsing. This command is not applicable to Foreign Exchange Station (FXS) voice ports because the ports do not generate out-dialing. This command also specifies the detection direction. Multifrequency tone dialing is not supported for FXS and FXO.

Voice ports can always detect DTMF and pulse signals. This command does not affect voice port dialing detection.

The **dial-type** command affects out-dialing as configured for the dial peer.

If you are using the **dial-type** command with E&M Wink Start signaling, use the **dtmf** or **mf** option.

SGCP 1.1+ does not support pulse dialing.

Examples

The following example shows a voice port configured to support a rotary (pulse tone) dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type pulse
```

The following example shows a voice port configured to support a DTMF (touch-tone) dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type dtmf
```

The following example shows a voice port configured to support a multifrequency tone dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type mf
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

dialer extsig

To configure an interface to initiate and terminate calls using an external signaling protocol, use the **dialer extsig** command in interface configuration mode. To discontinue control of the interface by the external signaling protocol, use the **no** form of this command.

dialer extsig

no dialer extsig

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	The command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5850.

Usage Guidelines

This command is used with the Network Access Server Package for Media Gateway Control Protocol feature. Configuring the **dialer in-band** command is a prerequisite to using this command. The configuration is blocked for profile dialers.

Examples

The following example shows output from the **dialer extsig** command:

```
Router(config)# interface Dialer1
Router(config-if)# dialer extsig
```

Related Commands

Command	Description
debug dialer	Provides debugging information for two types of dialer information: dial-on-demand events and dial-on-demand traffic.
dialer in-band	Specifies that DDR is to be supported.
extsig mgcp	Configures external signaling control by MGCP for a T1 or E1 trunk controller card.
show dialer	Displays dialer-related information for DNIS, interface, maps, and sessions.

dialer preemption level

To set the precedence for voice calls to be preempted by a dial-on demand routing (DDR) call for the dialer map, use the **dialer preemption level** command in map-class dialer configuration mode. To remove the preemption setting, use the **no** form of this command.

dialer preemption level {**flash-override | flash | immediate | priority | routine**}

no dialer preemption level {**flash-override | flash | immediate | priority | routine**}

Syntax Description

flash-override	Sets the precedence for DDR calls to preemption level 0 (highest).
flash	Sets the precedence for DDR calls to preemption level 1.
immediate	Sets the precedence for DDR calls to preemption level 2.
priority	Sets the precedence for DDR calls to preemption level 3.
routine	Sets the precedence for DDR calls to preemption level 4 (lowest). This is the default.

Command Default

The preemption level default is **routine** (lowest).

Command Modes

Map-class dialer configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following example sets a preemption level of *priority* (level 3) for the dialer map-class *dial1*.

```
Router(config)# map-class dialer dial1
Router(config-map-class)# dialer preemption level priority
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer trunkgroup	Defines the dial-on-demand trunk group label for the dialer interface.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
preemption enable	Enables preemption capabilities on a trunk group.

Command	Description
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.
preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

dialer trunkgroup

To define the dial-on-demand trunk group label for the dialer interface, use the **dialer trunkgroup** command in map-class dialer configuration mode. To remove the trunk group label, use the **no** form of this command.

dialer trunkgroup *label*

no dialer trunkgroup *label*

Syntax Description

label	Unique name for the dialer interface trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default No dialer trunk group is defined.

Command Modes Map-class dialer configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples The following example creates a trunk group named 20 for dialer map-class *dial1*.

```
Router(config)# map-class dialer dial1
Router(config-map-class)# dialer trunkgroup 20
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
show dialer	Displays general diagnostic information for interfaces configured for dial-on-demand routing (DDR).
trunk group	Defines a trunk group (global configuration) and enters trunk group configuration mode.

digit

To designate the number of digits for SCCP telephony control (STC) application feature speed-dial codes, use the **digit** command in STC application feature speed-dial configuration mode. To reset to the default, use the **no** form of this command.

digit *number*

no digit

Syntax Description

number	Number of digits for speed-dial codes. Values are 1 or 2. Default is 1.

Command Default

The default number of digits is 1.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used with the STC application, which enables features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

This command determines the number of digits that can be configured for speed-dial codes using the **speed dial** and **voicemail** commands. Use this command only if you want to change the number of digits from its default, which is 1. If you modify the value of this command, the **speed dial** and **voicemail** commands are reset to their defaults. If you set the value to 2 and then try to configure a single-digit speed-dial code, the system converts the speed-dial code into two digits.

Note that the phone numbers that are stored with various speed-dial codes are configured on the call-control device, such as Cisco CallManager or a Cisco CallManager Express router.

Examples

The following example sets the number of digits for speed-dial codes to two. It also sets a speed-dial prefix of one pound sign (#) and a speed-dial code range from 5 to 25. After these values are configured, a phone user presses #10 on the keypad to dial the number that was stored with code 10.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix #
Router(stcapp-fsd)# digit 2
Router(stcapp-fsd)# speed dial from 5 to 25
```

Related Commands

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
show stcapp feature codes	Displays configured and default STC application feature access codes.
speed dial	Designates a range of STC application feature speed dial codes.
voicemail	Designates an STC application feature speed-dial code to dial the voice-mail number.

digit-strip

To enable digit stripping on a plain old telephone service (POTS) dial-peer call leg, use the **digit-strip** command in dial peer configuration mode. To disable digit stripping on the dial-peer call leg, use the **no** form of this command.

digit-strip

no digit-strip

Syntax Description

This command has no arguments or keywords.

Command Default

Digit stripping is enabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: • VoIP (Cisco 2600 series, Cisco 3600 series, Cisco MC3810) • Voice over Frame Relay (VoFR)—Cisco 2600 series, Cisco 3600 series, Cisco MC3810) • Voice over ATM (VoATM)—Cisco 3600 series and Cisco MC3810.
12.1(1)T	This command was integrated in Cisco IOS Release 12.1(1)T
12.1(2)T	This command was first implemented in Cisco IOS Release 12.1(2)T for the following voice technologies on the following platforms: • VoIP (Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series, Cisco MC3810)

Usage Guidelines

The **digit-strip** command is supported on POTS dial peers only.

When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface.

Table 21 lists a series of dial peers configured with a specific destination pattern and shows the longest matched number after the digit is stripped based on the dial string 408 555-3048.

Table 21 Dial Peer Configurations with Longest Matched Number

Dial Peer	Destination Pattern	Preference	Session Target	Longest Matched Number
1	4085553048	0 (highest)	100-voip	10
2	408[0-9]553048	0	200-voip	9
3	408555	0	300-voip	6
4	408555	1(lower)	400-voip	6
5	408%	1	500-voip	3
6	.....	0	600-voip	0
7	.....	1	1:D (interface)	0

Table 22 lists a series of dial peers configured with a specific destination pattern and shows the number after the digit strip based on the dial string 408 555-3048 and the different dial-peer symbols applied.

Table 22 Dial Peer Configurations with Digits Stripped

Dial Peer	Destination Pattern	Number After the Digit Strip
1	408555....	3048
2	408555.%	3048
3	408525.+	3048
4	408555.?	3048
5	408555+	3048
6	408555%	53048
7	408555?	53048
8	408555[0-9].%	3048
9	408555(30).%	3048
10	408555(30)%	3048
11	408555..48	3048

Examples

The following example disables digit stripping on a POTS dial peer:

```
dial-peer voice 100 pots
 no digit-strip
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.

Command	Description
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

digital-filter

To specify the digital filter to be used before the voice packet is sent from the digital signal processor (DSP) to the network, use the **digital-filter** command in voice-class configuration mode. To remove the digital filter, use the **no** form of this command.

digital-filter {**1950hz** | **2175hz**}

no digital-filter {**1950hz** | **2175hz**}

Syntax Description

1950hz	Filter out 1950 Hz frequency.
2175hz	Filter out 2175 Hz frequency.

Command Default Digital filtering is disabled.

Command Modes Voice-class configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines The **digital-filter** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). The digital filter improves voice quality by preventing transmission of the guard tone with the voice packet from the LMR system to the VoIP network. The guard tone is configured with the **inject guard-tone** command. The digital filter can be configured to filter out either 2175 Hz or 1950 Hz. Only one of these frequencies can be filtered out at a time. Filtering is performed by the DSP.

Examples The following example specifies that 1950 Hz guard tone be filtered out of the voice packet before it is sent from the DSP to the network:

```
voice class tone-signal mytones
 digital-filter 1950hz
```

Related Commands

Command	Description
inject guard-tone	Plays out a guard tone with the voice packet.

direct-inward-dial

To enable the direct inward dialing (DID) call treatment for an incoming called number, use the **direct-inward-dial command in** dial peer configuration mode. To disable DID on the dial peer, use the **no** form of this command.

direct-inward-dial

no direct-inward-dial

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced.
12.0(4)T	This command was modified for store-and-forward fax.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use the **direct-inward-dial** command to enable the DID call treatment for an incoming called number. When this feature is enabled, the incoming call is treated as if the digits were received from the DID trunk. The called number is used to select the outgoing dial peer. No dial tone is presented to the caller.

Use the **no** form of this command to disable DID on the dial peer. When disabled, the called number is used to select the outgoing dial peer. The caller is prompted for a called number via dial tone.

This command is applicable only to plain old telephone service (POTS) dial peers. This command applies to on-ramp store-and-forward fax functions.

Examples

The following example enables DID call treatment for the incoming called number:

```
dial-peer voice 10 pots
  direct-inward-dial
```

disable-early-media 180

To specify which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP), use the **disable-early-media 180** command in sip-ua configuration mode. To enable early media cut-through for 180 messages with SDP, use the **no** form of this command.

disable-early-media ***180***

no disable-early-media ***180***

Syntax Description

This command has no arguments or keywords.

Command Default

Early media cut-through for 180 responses with SDP is enabled.

Command Modes

SIP-UA configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command provides the ability to enable or disable early media cut-through on Cisco IOS gateways for Session Initiation Protocol (SIP) 180 responses with SDP. Use the **disable-early-media 1*80*** *command to configure the gateway to ignore the SDP message and provide local ringback.* To restore the default treatment, early media cut-through, use the **no disable-early-media** ***180*** *command.*

Examples

The following example disables early media cut-through for SIP 180 responses with SDP:

```
Router(config-sip-ua)# disable-early-media 180
```

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP-UA timers.
sip-ua	Enables the SIP-UA configuration commands.

disc_pi_off

To enable an H.323 gateway to disconnect a call when it receives a disconnect message with a progress indicator (PI) value, use the **disc_pi_off** command in voice-port configuration mode. To restore the default state, use the **no** form of this command.

disc_pi_off

no disc_pi_off

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway does not disconnect a call when it receives a disconnect message with a PI value.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco 7500 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **disc_pi_off** voice-port command is valid only if the disconnect with PI is received on the inbound call leg. For example, if this command is enabled on the voice port of the originating gateway, and a disconnect message with PI is received from the terminating switch, the disconnect message is converted to a disconnect message. But if this command is enabled on the voice port of the terminating gateway, and a disconnect message with PI is received from the terminating switch, the disconnect message is not converted to a standard disconnect message because the disconnect message is received on the outbound call leg.

Note The **disc_pi_off** voice-port configuration command is valid only for the default session application; it does not work for interactive voice response (IVR) applications.

Examples

The following example handles a disconnect message with a PI value in the same way as a standard disconnect message for voice port 0:23:

```
voice-port 0:D
 disc_pi_off
```

Related Commands

Command	Description
isdn t306	Sets a timer for Disconnect messages.

disconnect-ack

To configure a Foreign Exchange Station (FXS) voice port to return an acknowledgment upon receipt of a disconnect signal, use the **disconnect-ack** command in voice-port configuration mode. To disable the acknowledgment, use the **no** form of this command.

disconnect-ack

no disconnect-ack

Syntax Description This command has no arguments or keywords.

Command Default FXS voice ports return an acknowledgment upon receipt of a disconnect signal

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines The **disconnect-ack** command configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first.

Examples The following example, which begins in global configuration mode, turns off the disconnect acknowledgment signal on voice port 1/1/0:

```
voice-port 1/0/0
 no disconnect-ack
```

Command History

Command	Description
show voice port	Displays voice port configuration information.

dnis (DNIS group)

To add a dialed number identification service (DNIS) number to a DNIS map, use the **dnis** command in DNIS-map configuration mode. To delete a DNIS number, use the **no** form of this command.

dnis *number* [**url** *url*]

no dnis

Syntax Description

number	Adds a user-selected DNIS number to a DNIS map.
url *url*	(Optional) URL that links a DNIS number to a specific VoiceXML document. If a URL is not entered, the DNIS number is linked to the VoiceXML application in the dial peer, which must be configured using the **application** command. This keyword is not valid for Tool Command Language (TCL) applications.

Command Default

If no URL is entered, the DNIS number links to the VoiceXML application that is configured in the dial peer with the **application** command.

Command Modes

DNIS-map configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

To enter DNIS-map configuration mode for the **dnis** command, use the **voice dnis-map** command.

Enter the **dnis** command once for each telephone number that you want to map to a voice application. A separate entry must be made for each telephone number in a DNIS map. Wildcards are not supported.

URLs in DNIS entries are used only by VoiceXML applications. When an incoming called number matches a DNIS entry, it loads the VoiceXML document that is specified by the URL, provided that a VoiceXML application is configured in the dial peer using the **application** command.

Non-VoiceXML applications, such as TCL applications, ignore the URLs in DNIS maps and link a call to the TCL application that is configured in the dial peer using the **application** command.

For a DNIS map to be applied to an outbound dial peer, a VoiceXML application must be configured by using the **application** command with the **out-bound** keyword. Otherwise, the call is not handed off to the application that is specified in the URL of the DNIS map.

The number of allowable DNIS entries is limited by the amount of available configuration memory on the gateway. As a guideline, DNIS maps that contain more than several hundred DNIS entries should be maintained in an external text file.

To associate a DNIS map with a dial peer, use the **dnis-map** command.

Examples

The first line in the following example shows how the **voice dnis-map** command is used to create a DNIS map named "dmap1". The last two lines show how the **dnis** command is used to enter DNIS entries.

The first DNIS entry specifies the location of a VoiceXML document. The second DNIS entry does not specify a URL. A DNIS number without a URL is, by default, matched to the URL of the application that is configured in the dial peer by using the **application** command.

```
voice dnis-map dmap1
 dnis 5553305 url tftp://blue/sky/test.vxml
 dnis 5558888
```

Related Commands

Command	Description
dnis-map	Associates a DNIS map with a dial peer.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map	Enters DNIS map configuration mode to create a DNIS map.
voice dnis-map load	Reloads a DNIS map that has changed since the previous load.

dnis-map

To associate a dialed number identification service (DNIS) map with a dial peer, use the **dnis-map** command in dial peer configuration mode. To remove a DNIS map from the dial peer, use the **no** form of this command.

dnis-map *map-name*

no dnis-map

Syntax Description

map-name	Name of the configured DNIS map.

Command Default No default behavior or values

Command Modes Dial peer configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines A DNIS map is a table of destination numbers with optional URLs that link to specific VoiceXML documents. When configured in a dial peer, a DNIS map enables you to link multiple called numbers to a single Tool Command Language (TCL) application or to individual VoiceXML documents.

The **dnis-map** command must be used with the **application** command.

Only one DNIS map can be configured in each dial peer.

To create a DNIS map, use the **voice dnis-map** command to enter DNIS-map configuration mode, and then use the **dnis** command to add entries to the DNIS map. Or you can create an external text file of DNIS entries and link to its URL by using the **voice dnis-map** command.

To view the configuration information for DNIS maps, use the **show voice dnis-map** command.

A URL configured for a DNIS number is ignored by a TCL application; the TCL script that is configured for the application is used instead.

Note For a DNIS map to be applied to an outbound dial peer, the call application must be configured as an outbound application. That is, a VoiceXML application must be configured by using the **application** command with the **out-bound** keyword. Otherwise, the call is not handed off to the application that is specified in the URL of the DNIS map.

Examples

In the following example the DNIS map named “dmap1” is associated with the VoIP dial peer 3. The outbound application “vapptest1” is associated through this dial peer with DNIS map “dmap1”.

```
dial-peer voice 3 voip
 dnis-map dmap1
 application vapptest1 outbound
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map	Enters DNIS map configuration mode to create a DNIS map.
voice dnis-map load	Reloads a DNIS map that has changed since the previous load.

domain-name (annex G)

To set the domain name that is reported in service relationships, use the **domain-name** command in annex G neighbor configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *id*

no domain-name *id*

Syntax Description

id	Domain name that is reported in service relationships.

Command Modes

Annex G neighbor configuration mode

Command Default

No default behavior or values

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to set the domain name reported that is reported in service relationships.

Examples

The following example shows how to set a domain name to “boston1”:

```
Router(config-annexg-neigh)# domain-name boston1
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.

drop-last-conferee

To define a Feature Access Code (FAC) to access the Drop Last Conferee feature in feature mode on analog phones controlled by Cisco Unified Communications Manager Express (CME), use the **drop-last-conferee** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

drop-last-conferee *keypad-character*

no drop-last-conferee

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0—9, *, #). Default is #4.

Command Default

The default value is #4.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for the Drop Last Conferee feature from the default (#4) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Note This command does not change the user experience for Drop Last Conferee if the Cisco call-control system is Cisco Unified Communications Manager.

Examples

The following example shows how to change the value of the feature code for the Drop Last Conferee feature from the default (#4). With this configuration, a phone user in a three-party conference on an analog phone controlled by Cisco Unified CME presses hook flash to get the feature tone and then dials 44 to drop the last active party. The conference becomes a basic call to the second call party.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# drop-last-conferee 44
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

ds0 busyout (voice)

To force a DS0 time slot on a controller into the busyout state, use the **ds0 busyout command in** controller configuration mode. To remove the DS0 time slot from the busyout state, use the **no** form of this command.

ds0 busyout *ds0-time-slot*

no ds0 busyout *ds0-time-slot*

Syntax Description

ds0-time-slot	DS0 time slots to be forced into the busyout state. Range is from 1 to 24 and can include any combination of time slots.

Command Default DS0 time slots are not in busyout state.

Command Modes Controller configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on Cisco MC3810 and Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines The **ds0 busyout** command affects only DS0 time slots that are configured into a DS0 group and that function as part of a digital voice port. If multiple DS0 groups are configured on a controller, any combination of DS0 time slots can be busied out, provided that each DS0 time slot to be busied out is part of a DS0 group.

If a DS0 time slot is in the busyout state, only the **no ds0 busyout** command can restore the DS0 time slot to service.

To avoid conflicting command-line interface (CLI) commands, do not use the **ds0 busyout** command and the **busyout forced** command on the same controller.

Examples The following example configures DS0 time slot 6 on controller T1 0 to be forced into the busyout state:

```
controller t1 0
 ds0 busyout 6
```

The following example configures DS0 time slots 1, 3, 4, 5, 6, and 24 on controller E1 1 to be forced into the busyout state:

```
controller e1 1
 ds0 busyout 1,3-6,24
```

Related Commands

Command	Description
busyout seize	Changes the busyout seize procedure for a voice port.
show running configuration	Determines which DS0 time slots have been forced into the busyout state.

ds0-group (E1)

To specify the DS0 time slots that make up a logical voice port on an E1 controller, specify the signaling type by which the router communicates with the PBX or PSTN, and define E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, use the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

Cisco IOS Release 12.2 and Later Releases

Cisco 1750 and Cisco 1751

ds0-group *ds0-group-number* **timeslots** *timeslot-list {*[**service** *service-type*] | [**type** **e&m-fgb | e&m-fgd | e&m-immediate-start | fgd-eana | fgd-os | fxs-ground-start | fxs-loop-start | none | r1-itu | r1-modified | r1-turkey**]}

no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases

Cisco 1750 and Cisco 1751

ds0-group *ds0-group-number* **timeslots** *timeslot-list {*[**service** *service-type*] | [**type** **e&m-fgb | e&m-fgd | e&m-immediate-start | fgd-eana | fgd-os | fxs-ground-start | fxs-loop-start | none | r1-itu | r1-modified | r1-turkey | sas-ground-start | sas-loop-start**]}

no ds0-group *ds0-group-number*

Cisco 2600 Series (Except Cisco 2691), Cisco 3600 Series (Except Cisco 3660)

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial | e&m-immediate-start | e&m-melcas-delay | e&m-melcas-immed | e&m-melcas-wink | e&m-wink-start | ext-sig | fgd-eana | fxo-ground-start | fxo-loop-start | fxo-melcas | fxs-ground-start | fxs-loop-start | fxs-melcas | r2-analog | r2-digital | r2-pulse**}

no ds0-group *ds0-group-number*

Cisco 2691, Cisco 2600XM Series, Cisco 2800 Series (Except Cisco 2801), Cisco 3660, Cisco 3700 Series, Cisco 3800 Series

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial | e&m-immediate-start | e&m-lmr | e&m-melcas-delay | e&m-melcas-immed | e&m-melcas-wink | e&m-wink-start | ext-sig | fgd-eana | fxo-ground-start | fxo-loop-start | fxo-melcas | fxs-ground-start | fxs-loop-start | fxs-melcas | r2-analog | r2-digital | r2-pulse**}

no ds0-group *ds0-group-number*

Cisco 7200 Series and Cisco 7500 Series Voice Ports

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial | e&m-fgd | e&m-immediate-start | e&m-wink-start | fxo-ground-start | fxo-loop-start | fxs-ground-start | fxs-loop-start** }

no ds0-group *ds0-group-number*

Cisco 7700 Series Voice Ports

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-wink-start** | **fxs-ground-start** | **fxs-loop-start** | **fxo-ground-start** | **fxo-loop-start**}

no ds0-group *ds0-group-number*

Cisco AS5300 and the Cisco AS5400

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**none** | **p7** | **r2-analog** | **r2-digital** | **r2-lsv181-digital** | **r2-pulse**}

no ds0-group *ds0-group-number*

Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5x00 series.

Syntax Description

ds0-group-number	A value that identifies the DS0 group. Range is from 0 to 14 and 16 to 30; 15 is reserved.
timeslots *timeslot-list*	Lists time slots in the DS0 group. The *timeslot-list* argument is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. Range is from 1 through 31. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12
type	Specifies the type of signaling for the DS0 group. The signaling method selection for the **type** keyword depends on the connection that you are making. The ear and mouth (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The Foreign Exchange Station (FXS) interface allows connection of basic telephone equipment and PBX. The Foreign Exchange Office (FXO) interface is for connecting the central office (CO) to a standard PBX interface where permitted by local regulations; it is often used for off-premise extensions (OPXs). Types are as follows: • **e&m-delay-dial**—The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination. • **e&m-fgb**—E&M Type II Feature Group B. • **e&m-fgd**—E&M Type II Feature Group D. • **e&m-immediate-start**—E&M immediate start. • **e&m-lmr**—E&M Land Mobile Radio (LMR). • **e&m-melcas-delay**—E&M MELCAS delay-start signaling support. • **e&m-melcas-immed**—E&M MELCAS immediate-start signaling support.

	• **e&m-melcas-wink**—E&M MELCAS wink-start signaling support. • **e&m-wink-start**—The originating endpoint sends an off-hook signal and waits for a wink-start from the destination. • **fgd-eana—Feature Group D exchange access North American.** • **fgd-os**—Feature Group D operator services. • **fxo-ground-start—FXO ground-start signaling.** • **fxo-loop-start—FXO loop-start signaling.** • **fxo-melcas—FXO MELCAS signaling.** • **fxs-ground-start—FXS ground-start signaling.** • **fxs-loop-start—FXS loop-start signaling.** • **fxs-melcas—FXS MELCAS signaling.** • **none**—Null signaling for external call control. • **p7**—Specifies the p7 switch type. • **r1-itu**—Line signaling based on international signaling standards. • **r1-modified**—An international signaling standard that is common to channelized T1/E1 networks. • **r1-turkey**—A signaling standard used in Turkey. • **r2-analog—R2 analog line signaling.** • **r2-digital—R2 digital line signaling.** • **r2-lsv181-digital**—Specifies a specific R2 digital line. • **r2-pulse—7-pulse line signaling, a transmitted pulse that indicates a change in the line state.** • **sas-ground-start—Single attachment station (SAS) ground-start.** • **sas-loop-start—SAS loop-start.**
service *service-type*	(Optional) Specifies the type of service. • **data**—data service • **fax**— store-and-forward fax service • **voice**—voice service (for FGD-OS service) • **mgcp**—Media Gateway Control Protocol service

Command Default There is no DS0 group. Calls are allowed in both directions.

Command Modes Controller configuration

Command History

Release	Modification
11.2	This command was introduced for the Cisco AS5300 as the **cas-group** command.
11.3(1)MA	The command was introduced as the **voice-group** command for the Cisco MC3810.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the **cas-group** command was implemented on the Cisco 3600 series routers.
12.0(5)T	The command was renamed **ds0-group** on the Cisco AS5300 and Cisco 2600 series and Cisco 3600 series routers. Some keyword modifications were implemented.
12.0(5)XE	This command was implemented on the Cisco 7200 series.
12.0(7)XK	Support for this command was implemented on the Cisco MC3810. When the **ds0-group** command became available on the Cisco MC3810, the **voice-group** command was removed and no longer supported. The **ext-sig** keyword replaced the **ext-sig-master** and **ext-sig-slave** keywords that were available with the **voice-group** command.
12.0(7)XR	The **mgcp** service type was added.
12.1(2)XH	The **e&m-fgd** and **fgd-eana** keywords were added for Feature Group D signaling.
12.1(5)XM	The **sgcp** keyword was removed.
12.1(3)T	This command was modified for Cisco 7500 series routers. The **fgd-os** signaling type and the **voice** service type were added.
12.2	The command was modified to exclude **sas** keywords**.** The Single Attachment Station (SAS) CAS options of **sas-loop-start** and **sas-ground-start** are not supported as a type of signaling for the DS0 group.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(2)XN	Support for the **mgcp** keyword was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was supported with Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command is supported on the Cisco IAD2420 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850 in this release.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The Cisco 1750 and Cisco 1751 do not support T1 and E1 voice and data cards in Cisco IOS Release 12.2(13)T. The Cisco 17xx platforms can support only HC DSP firmware images in this release.

Release	Modification
12.3(8)T	Documentation of the **ds0-group** command was divided into the individual **ds0-group (E1)** and **ds0-group (T1)** commands.
12.4(2)T1	Support was added for the **e&m-lmr** signaling type on the Cisco 2691, Cisco 2600XM series, Cisco 2800 series (except Cisco 2801), Cisco 3660, Cisco 3700 series, and Cisco 3800 series.

Usage Guidelines

The **ds0-group** command automatically creates a logical voice port that is numbered as follows:

- Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745, and Cisco 7200 series:
  - *slot*/*port*:*ds0-group-number*

Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Be sure you take the following into account when you are configuring DS0 groups:

- Channel groups, CAS voice groups, DS0 groups, and time-division multiplexing (TDM) groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, DS0 groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.
- The keywords available for the **ds0-group** command are dependent upon the Cisco IOS software release that you are using. For the most current information, go to the Cisco Feature Navigator home page at the following URL:
  http://www.cisco.com/go/fn
- When you are using command-line interface (CLI) help, the keywords for the **ds0-group** command are configuration specific. For example, if Media Gateway Control Protocol (MGCP) is configured, you see the **mgcp** keyword. If you are not using MGCP, you do not see the **mgcp** keyword.
- Cisco IOS Releases later than 12.2 do not support the Single Attachment Station (SAS) CAS options of sas-loop-start and sas-ground-start.

Examples

The following example shows ranges of E1 controller time slots configured for FXS ground-start and FXO loop-start signaling:

```
E1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-10 type fxs-ground-start
 ds0-group 2 timeslots 11-24 type fxo-loop-start
```

The following example shows ranges of T1 controller time slots configured for FXS ground-start signaling:

```
controller E1 1/0
 ds0-group 1 timeslots 1-4 type fxs-ground-start
```

The following example illustrates setting the E1 channels for Signaling System 7 (SS7) service on any trunking gateway using the **mgcp** keyword:

```
Router(config-controller)# ds0-group 0 timeslots 1-24 type none service mgcp
```

In the following example, the time slot maximum is 12 and the time slot is 1, so two voice-ports are created successfully.

```
controller E1 0/0
 ds0-group 0 timeslots 1-4 type e&m-immediate-start
 ds0-group 1 timeslots 6-12 type e&m-immediate-start
```

If a third DS0 group is added, the voice-port is rejected even though the total number of voice channels is less than 16.

```
 ds0-group 2 timeslots 17-18 type e&m-immediate-start
```

In the following example, the signaling type is set to e&m-lmr:

```
ds0-group 0 timeslots 1-10 type e&m-lmr
```

Related Commands

Command	Description
cas-group	Configures channelized T1 time slots with robbed bit signaling.
codec	Specifies the voice coder rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard that you are using.

ds0-group (T1)

To specify the DS0 time slots that make up a logical voice port on a T1 controller, to specify the signaling type by which the router communicates with the PBX or PSTN, and to define T1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, use the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

Cisco IOS Release 12.2 and Later Releases

Cisco 1750 and Cisco 1751

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey**}

no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases

Cisco 1750 and Cisco 1751

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey** | **sas-ground-start** | **sas-loop-start**}

no ds0-group *ds0-group-number*

Cisco 2600 Series (Except Cisco 2691), Cisco 3600 Series (Except Cisco 3660), and Cisco VG 200

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}

no ds0-group *ds0-group-number*

Cisco 2691, Cisco 2600XM Series, Cisco 2800 Series (Except Cisco 2801), Cisco 3660, Cisco 3700 Series, Cisco 3800 Series

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** | **e&m-lmr** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fgd-emf** [**mf**] [**ani-pani**] [**ani**] | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}

no ds0-group *ds0-group-number*

Cisco 7200 Series and Cisco 7500 Series

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** | **e&m-wink-start** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}

no ds0-group *ds0-group-number*

Cisco 7700 Series Voice Ports

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-wink-start** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}

no ds0-group *ds0-group-number*

Cisco IOS Release 12.2 and Later Releases

Cisco AS5300, Cisco AS5350, and Cisco AS5400

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type** [**e&m-fgb** [**dtmf** | **mf**] | **e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**]| **none**]]

no ds0-group *ds0-group-number*

Cisco AS5850

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type** [**e&m-fgb** [**dtmf** | **mf**] | **e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **r1-itu** [**dnis**] | **none**]]

no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases

Cisco AS5300, Cisco AS5350, and Cisco AS5400

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type** [**e&m-fgb** [**dtmf** | **mf**] | **e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **sas-ground-start** | **sas-loop-start** | **none**]]

no ds0-group *ds0-group-number*

Cisco AS5850

ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type** [**e&m-fgb** [**dtmf** | **mf**] | **e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **r1-itu** [**dnis**] | **sas-ground-start** | **sas-loop-start** | **none**]]

no ds0-group *ds0-group-number*

Syntax Description

ds0-group-number	A value that identifies the DS0 group. Range is from 0 to 23.
timeslots *timeslot-list*	Lists time slots in the DS0 group. The *timeslot-list* argument is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. Range is from 1 to 24. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12
• **typenone**—Null signaling for external call control.	Specifies the type of signaling for the DS0 group. The signaling method selection for the **type** keyword depends on the connection that you are making. The ear and mouth (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The Foreign Exchange Station (FXS) interface allows connection of basic telephone equipment and PBX. The Foreign Exchange Office (FXO) interface is for connecting the central office (CO) to a standard PBX interface where permitted by local regulations; it is often used for off-premise extensions (OPXs). Types are as follows: • **e&m-delay-dial**—The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination. • **e&m-fgb**—E&M Type II Feature Group B. • **e&m-fgd**—E&M Type II Feature Group D. • **e&m-immediate-start**—E&M immediate start. • **e&m-lmr**—E&M Land Mobile Radio (LMR). • **e&m-wink-start**—The originating endpoint sends an off-hook signal and waits for a wink-start from the destination. • **ext-sig**—The external signaling interface specifies that the signaling traffic comes from an outside source. • **fgd-eana—Feature Group D exchange access North American.** • **fgd-emf—**FGD Enhanced MF. • **fgd-os**—Feature Group D operator services. • **fxo-ground-start—FXO ground-start signaling.** • **fxo-loop-start—FXO loop-start signaling.** • **fxs-ground-start—FXS ground-start signaling.** • **fxs-loop-start—FXS loop-start signaling.** • **none**—Null signaling for external call control. • **r1-itu**—Line signaling based on international signaling standards. (This signaling type is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.) • **r1-modified**—An international signaling standard that is common to channelized T1/E1 networks.

	• **r1-turkey**—A signaling standard used in Turkey. • **sas-ground-start**—Single attachment station (SAS) ground-start. • **sas-loop-start**—SAS loop-start.
service *service-type*	(Optional) Specifies the type of service. • **data**—Data service. • **fax**— Store-and-forward fax service. • **mgcp**[1]—Media Gateway Control Protocol service. • **sccp**[1]—Simple Gateway Control Protocol service. • **voice**—Voice service (for FGD-OS service).
dtmf	(Optional) Specifies dual tone multifrequency (DTMF) tone signaling.
mf	(Optional) Specifies multifrequency (MF) tone signaling
ani	(Optional) Provisions ANI address information.
ani-dnis	(Optional) Specifies automatic number identification (ANI) and dialed number identification service (DNIS) address information provisioning for FGD OS.
ani-pani	(Optional) Provisions ANI and PANI address information.
dnis-ani	(Optional) Specifies ANI and DNIS address information provisioning for FGD EANA.
dnis	(Optional) Specifies DNIS address information provisioning.
info-digits-no-strip	(Optional) Retains info digits on the Cisco AS5x00 platforms.

1. Used only with the **type none** keywords on the Cisco AS5x00 platforms.

Command Default There is no DS0 group. Calls are allowed in both directions.

Command Modes Controller configuration

Command History

Release	Modification
11.2	This command was introduced for the Cisco AS5300 as the **cas-group** command.
11.3(1)MA	The command was introduced as the **voice-group** command for the Cisco MC3810.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the **cas-group** command was implemented on the Cisco 3600 series routers.
12.0(5)T	The command was renamed **ds0-group** on the Cisco AS5300 and Cisco 2600 series and Cisco 3600 series routers. Some keyword modifications were implemented.
12.0(5)XE	This command was implemented on the Cisco 7200 series.

Release	Modification
12.0(7)XK	Support for this command was implemented on the Cisco MC3810. When the **ds0-group** command became available on the Cisco MC3810, the **voice-group** command was removed and no longer supported. The **ext-sig** keyword replaced the **ext-sig-master** and **ext-sig-slave** keywords that were available with the **voice-group** command.
12.0(7)XR	The **mgcp** service type was added.
12.1(2)XH	The **e&m-fgd** and **fgd-eana** keywords were added for Feature Group D signaling.
12.1(5)XM	The **sgcp** keyword was removed.
12.1(3)T	This command was modified for Cisco 7500 series routers. The **fgd-os** signaling type and the **voice** service type were added.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2	The command was modified to exclude **sas** keywords**.** The Single Attachment Station (SAS) CAS options of **sas-loop-start** and **sas-ground-start** are not supported as a type of signaling for the DS0 group.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(2)XN	Support for the **mgcp** keyword was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was supported in Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command is supported on the Cisco IAD2420 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850 in this release.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The Cisco 1750 and Cisco 1751 do not support T1 and E1 voice and data cards in Cisco IOS Release 12.2(13)T. The Cisco 17xx platforms can support only HC DSP firmware images in this release.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 3725, and Cisco 3745.
12.3(4)XD	This command was modified for the Cisco 3725 and Cisco 3745. The **e&m-lmr** signaling type was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T	Documentation of the **ds0-group** command was divided into the individual **ds0-group (E1)** and **ds0-group (T1)** commands.

Release	Modification
12.3(10)	The **info-digits-no-strip** keyword was added for use on the Cisco AS5x00 platforms.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T. The **fgd-emf**, **ani-pani**, and **ani** keywords were added for the Cisco 2800 and Cisco AS5x00 platforms.

Usage Guidelines

The **ds0-group** command automatically creates a logical voice port that is numbered as follows:

- Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 7200 series:
  - *slot*/*port*:*ds0-group-number*
- Cisco AS5300, Cisco AS5350, and Cisco AS5400 with a T1 controller:
  - *slot*/*port*
- Cisco AS5850 with a T1 controller:
  - *slot*/*port*:*ds0-group-number*

Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Be sure that you take the following into account when you are configuring DS0 groups:

- Channel groups, CAS voice groups, DS0 groups, and time-division multiplexing (TDM) groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, DS0 groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.
- The keywords available for the **ds0-group** command are dependent upon the Cisco IOS software release that you are using. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

  http://www.cisco.com/go/fn
- When you are using command-line interface (CLI) help, the keywords for the **ds0-group** command are configuration specific. For example, if Media Gateway Control Protocol (MGCP) is configured, you see the **mgcp** keyword. If you are not using MGCP, you do not see the **mgcp** keyword.

Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5x00 series.

Note The signaling type R1-ITU is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

Examples

The following example shows ranges of T1 controller time slots configured for FXS ground-start and FXO loop-start signaling:

```
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-10 type fxs-ground-start
 ds0-group 2 timeslots 11-24 type fxo-loop-start
```

The following example shows ranges of T1 controller time slots configured for FXS ground-start signaling:

```
controller T1 1/0
 ds0-group 1 timeslots 1-4 type fxs-ground-start
```

The following example illustrates setting the T1 channels for Signaling System 7 (SS7) service on any trunking gateway using the **mgcp** keyword:

```
ds0-group 0 timeslots 1-24 type none service mgcp
```

In the following example, the time slot maximum is 12 and the time slot is 1, so two voice-ports are created successfully.

```
controller T1 0/0
 ds0-group 0 timeslots 1-4 type e&m-immediate-start
 ds0-group 1 timeslots 6-12 type e&m-immediate-start
```

If a third DS0 group is added, the voice port is rejected even though the total number of voice channels is less than 16.

```
 ds0-group 2 timeslots 17-18 type e&m-immediate-start
```

In the following example, the signaling type is set to E&M LMR:

```
 ds0-group 0 timeslots 1-10 type e&m-lmr
```

You have the option to retain info digits when you are configuring E&M Type II Feature Group D with MF signaling and ANI/DNIS for calls being sent over IP. Info digits denote the subscriber type, and the info-digits keyword prepends info digits to the calling number.

On inbound calls from a T1 FGD voice-port with MF ANI-DNIS, when ANI information is obtained, it is passed unaltered to the next matching dial peer, either POTS or VoIP. The addition of the **info-digits-no-strip** keyword allows you to retain the info digits portion of the ANI information; the modified ANI is then passed to the next matching dial peer. Ordinarily, info digits are not valid for calls going over IP and are, therefore, stripped off. The ability to retain info digits is particularly useful for calls that are not leaving the PSTN network and are just being hairpinned back.

In the following example, the E&M Type II Feature Group D is configured with MF signaling and ANI/DNIS over IP while retaining info digits:

```
 ds0-group 0 timeslots 1-24 type e&m-fgd mf ani-dnis info-digits-no-strip
```

The following example enables FGD EMF:

```
 ds0-group 11 timeslots 11 type fgd-emf ani
 ds0-group 11 timeslots 11 type fgd-emf ani-pani
```

Related Commands

Command	Description
cas-group	Configures channelized T1 time slots with robbed bit signaling.
codec	Specifies the voice coder rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard that you are using.

ds0-num

To add B-channel information in outgoing Session Initiation Protocol (SIP) messages, use the **ds0-num** command in SIP voice service configuration mode. To return to the default setting, use the **no** form of this command.

ds0-num

no ds0-num

Syntax Description

This command has no arguments or keywords.

Command Default

B channel information is disabled.

Command Modes

SIP voice service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command enables the SIP application to receive B-channel information of incoming ISDN calls. The B-channel information appears in the Via header of an Invite request and information acquired from the Via header can be used during call transfer or to route a call.

Examples

The following example adds B-channel information to outgoing SIP messages:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# ds0-num
```

Related Commands

Command	Description
sip	Enables SIP voice service configuration commands.
voice service voip	Specifies the voice encapsulation type as VoIP.

dsn

To specify that a delivery status notice (DSN) be delivered to the sender, use the **dsn** command in dial peer configuration mode. To cancel a specific DSN option, use the **no** form of this command.

dsn {**delay** | **failure** | **success**}

no dsn {**delay** | **failure** | **success**}

Syntax Description

delay	Defines the delay for each mailer.
failure	Requests that a failed message be sent to the FROM address. This is a default.
success	Requests that message be sent to the FROM address that the message was delivered successfully to the recipient.

Note In the absence of any other DSN settings (for example, **no dsn**, or a mailer in the path that does not support the DSN extension), a failure to deliver message always causes a nondelivery message to be generated. This nondelivery message is called a *bounce*.

Command Default The default is to send a nondelivery message in the event of a failure

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines When the **delay** keyword is selected, the next-hop mailer sends a message to the FROM address saying that the mail message was delayed. The definition of the **delay** keyword is made by each mailer and is not controlled by the sender. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

When the **failur**e keyword is selected, the next-hop mailer sends a message to the FROM address that the mail message delivery failed. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

When the **success** keyword is selected, the next-hop mailer sends a message to the FROM address saying that the mail message was successfully delivered to the recipient. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

This command is applicable to Multimedia Mail over Internet Protocol (MMoIP) dial peers.

DSNs are messages or responses that are automatically generated and sent to the sender or originator of an e-mail message by the Simple Mail Transfer Protocol (SMTP) server, notifying the sender of the status of the e-mail message. Specifications for DSN are described in RFC 1891, RFC 1892, RFC 1893, and RFC 1894.

The on-ramp DSN request is included as part of the fax-mail message sent by the on-ramp gateway when the matching MMoIP dial peer has been configured. The on-ramp DSN response is generated by the SMTP server when the fax-mail message is accepted. The DSN is sent back to the user defined by the **mta send mail-from** command. The off-ramp DSN is requested by the e-mail client. The DSN response is generated by the SMTP server when it receives a request as part of the fax-mail message.

Note DSNs are generated only if the mail client on the SMTP server is capable of responding to a DSN request.

Because the SMTP server generates the DSNs, you need to configure both **mail from:** and **rcpt to:** on the server for the DSN feature to work. For example:

```
mail from: <user@mail-server.company.com>
rcpt to: <fax=555-1212@company.com> NOTIFY=SUCCESS,FAILURE,DELAY
```

There are three different states that can be reported back to the sender:

- Delay—Indicates that the message was delayed in being delivered to the recipient or mailbox.
- Success—Indicates that the message was successfully delivered to the recipient or mailbox.
- Failure—Indicates that the SMTP server was unable to deliver the message to the recipient or mailbox.

Because these delivery states are not mutually exclusive, you can configure store-and-forward fax to generate these messages for all or any combination of these events.

DSN messages notify the sender of the status of a particular e-mail message that contains a fax TIFF image. Use the **dsn** command to specify which notification messages are sent to the user.

The **dsn** command allows you to select more than one notification option by reissuing the command and specifying a different notification option each time. To discontinue a specific notification option, use the **no** form of the command for that specific keyword.

If the **failure** keyword is not included when DSN is configured, the sender receives no notification of message delivery failure. Because a failure is usually significant, care should be taken to always include the **failure** keyword as part of the **dsn** command configuration.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies that a DSN message be returned to the sender when the e-mail message that contains the fax has been successfully delivered to the recipient or if the message that contains the fax has failed to be delivered:

```
dial-peer voice 10 mmoip
 dsn success
 dsn failure
```

Related Commands

Command	Description
mta send mail-from hostname	Specifies the originator (host-name portion) of the e-mail fax message.
mta send mail-from username	Specifies the originator (username portion) of the e-mail fax message.

dsp allocation signaling dspid

To change the digital signal processor (DSP) selection for signaling channel allocation from the default (DSP weight-based) to the DSP ID number, use the **dsp allocation signaling dspid** command in voice-card configuration mode. To return to the default behavior, use the **no** form of this command.

dsp allocation signaling dspid

no dsp allocation signaling dspid

Syntax Description

This command has no arguments or keywords.

Command Default

Selection of a DSP for signaling channel allocation is based on the internal weighted value assigned to the DSPs.

Command Modes

Voice-card configuration (config-voicecard)

Command History

Release	Modification
12.4(15)T9	This command was introduced.

Usage Guidelines

The **dsp allocation signaling dspid** command takes effect only after a reload of the router. The command should be enabled and saved into the startup-config file.

The default signal channel allocation method (by weight) may not be suitable for some network implementations. The default allocation method selects the DSPs based on the DSP weight, and you cannot control the selection of the DSP for specific configuration even if the order of the packet voice data modules (PVDMs) is changed. Enable the **dsp allocation signaling dspid** command to change the selection order to the DSP ID number. This command is more useful when there is a PVDM2-8 module in the network configuration.

Examples

The following example shows how to change the default for DSP allocation from the DSP weight to the DSP ID number:

```
voice card 1
 dsp allocation signaling dspid
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels.
voice-card	Enters voice-card configuration mode.

dsp services dspfarm

To enable digital-signal-processor (DSP) farm services for a particular voice network module, use the **dsp services dspfarm** command in voice card configuration mode. To disable services, use the **no** form of this command.

dsp services dspfarm

no dsp services dspfarm

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Voice-card configuration (config-voicecard)

Command History

Release	Modification
12.2(13)T	This command was introduced.
Cisco IOS XE Release 3.2S	Support for this command was added on Cisco ASR 1000 Series Routers.

Usage Guidelines The router must be equipped with one or more voice network modules that provide DSP resources. DSP resources are used only if this command is configured under the particular voice card.

The number of voice network modules that must be enabled for DSP-farm services depends on the number of DSPs on the module and on the maximum number of transcoding and conferencing sessions configured for the DSP farm.

Note Use this command before enabling DSP-farm services with the **dspfarm** command for an NM-HDV or NM-HDV-FARM.

Cisco ASR 1000 Series Router

The SPA-DSPs on a Cisco ASR 1000 Series Routers are installed in a subslot on a SIP. Hence, when referring to a SPA-DSP the **voice-card** command is used.

Examples The following example enables DSP-farm services on an NM-HDV2 or NM-HD-1V/2V/2VE:

```
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

The following example enables DSP-farm services on an NM-HDV or NM-HDV-FARM:

```
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

The following example enables DSP-farm services on SPA-DSP for a Cisco ASR 1000 Series Router:

```
Router(config)# voice-card 1/1
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

Related Commands

Command	Description
dsp services dspfarm	Enables the DSP farm services.
dspfarm profile	Enters the DSP farm profile configuration mode, and defines a profile for the DSP farm services.
show voice dsp (SPA-DSP)	Displays the DSP current status or the selective statistics of the DSP voice channels.

dspfarm (DSP farm)

To enable digital-signal-processor (DSP) farm service, use the **dspfarm** command in global configuration mode. To disable the service, use the **no** form of this command.

dspfarm

no dspfarm

Syntax Description

This command has no arguments or keywords.

Command Default

DSP-farm service is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before enabling DSP-farm services, you must configure the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled using the **dsp service dspfarm** command. You must also specify the maximum number of transcoding sessions to be supported by the DSP farm using the **dspfarm transcoder maximum sessions** command.

This command causes the system to download new firmware into the DSPs, start up the required subsystems, and wait for a service request from the transcoding and conferencing applications.

Examples

The following example configures an NM-HDV or NM-HDV-FARM, specifies the maximum number of transcoding sessions, and enables DSP-farm services:

```
Router# configure terminal
Router(config)# no dspfarm
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
Router(config)# dspfarm transcoder maximum sessions 15
Router(config)# dspfarm
```

Related Commands

Command	Description
dsp services dspfarm	Specifies the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled.
dspfarm transcoder maximum sessions	Specifies the maximum number of transcoding sessions to be supported by a DSP farm.
show dspfarm	Displays summary information about DSP resources.

dspfarm (voice-card)

To add a specified voice card to those participating in a digital signal processor (DSP) resource pool, use the **dspfarm** command in voice-card configuration mode. To remove the specified card from participation in the DSP resource pool, use the **no** form of this command.

dspfarm

no dspfarm

Syntax Description

This command has no arguments or keywords.

Command Default

A card participates in the DSP resource pool

Command Modes

Voice-card configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced for the Cisco 3660.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	This command was implemented on the Cisco 2600 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 3725, and Cisco 3745.

Usage Guidelines

DSP mapping occurs when DSP resources on one AIM or network module are available for processing of voice time-division multiplexing (TDM) streams on a different network module or on a voice/WAN interface card (VWIC). This command is used on Cisco 3660 routers with multiservice interchange (MIX) modules installed or on Cisco 2600 series routers with AIMs installed.

To reach voice-card configuration mode for a particular voice card, from global configuration mode enter the **voice-card** command and the slot number for the AIM or network module that you want to add to the pool. See the **voice-card** command reference for details on slot numbering.

The assignment of DSP pool resources to particular TDM streams is based on the order in which the streams are configured with the **ds0-group** command for T1/E1 channel-associated signaling (CAS) or with the **pri-group** command for ISDN PRI.

The assignment of DSP pool resources does not occur dynamically during call signaling.

Examples

The following example adds to the DSP resource map the DSP resources on the network module in slot 5 on a Cisco 3660 with a MIX module:

```
voice-card 5
 dspfarm
```

The following example makes available the DSP resources on an AIM on a modular access router:

```
voice-card 0
 dspfarm
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller, to specify the signaling type by which the router communicates with the PBX or PSTN, and to define T1or E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN.
pri-group	Specifies ISDN Primary Rate Interface (PRI) on a channelized T1 or E1 controller.
voice-card	Enters voice-card configuration mode.

dspfarm confbridge maximum sessions

To specify the maximum number of concurrent conference sessions for which digital-signal-processor (DSP) farm resources should be allocated, use the **dspfarm confbridge maximum sessions** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm confbridge maximum sessions *number*

no dspfarm confbridge maximum sessions

Syntax Description

number	Number of conference sessions. A single DSP supports 1 conference session with up to 6 participants.

Command Default 0 sessions

Command Modes Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before using this command, you must disable DSP-farm service using the **no dspfarm** command.

The maximum number of conference sessions depends upon DSP availability in the DSP farm. A single DSP supports one conference session with up to six participants. However, you may need to allocate additional DSP resources for transcoding to support conferences. If all participants use G.711 or G.729 codecs, you need not allocate any additional DSP resources because transcoding is done in the conferencing DSP.

When you use this command, take into consideration the number of DSPs allocated for transcoding services with the **dspfarm transcoder maximum sessions** command.

Examples The following example sets the maximum number of conferencing sessions to 8:

```
Router# dspfarm confbridge maximum sessions 8
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm transcoder maximum sessions	Specifies the maximum number of transcoding sessions to be supported by a DSP farm.
show dspfarm	Displays summary information about DSP resources.

dspfarm connection interval

To specify the time interval during which to monitor Real-Time Transport Protocol (RTP) inactivity before deleting an RTP stream, use the **dspfarm connection interval** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm connection interval *seconds*

no dspfarm connection interval

Syntax Description

seconds	Interval, in seconds, during which to monitor RTP inactivity. Range is from 60 to 10800. Default is 600.

Command Default

600 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

After each interval, RTP streams are checked for inactivity. If all RTP streams for a particular call are inactive, the RTP timer, as set with the **dspfarm rtp timeout** command, is started. When the RTP timer expires, the call is deleted.

Examples

The following example sets the connection interval to 60 seconds:

```
Router(config)# dspfarm connection interval 60
```

Related Commands

Command	Description
dspfarm rtp timeout	Specifies the RTP timeout interval used to clear hanging connections.

dspfarm profile

To enter DSP farm profile configuration mode and define a profile for digital signal processor (DSP) farm services, use the **dspfarm profile** command in global configuration mode. To delete a disabled profile, use the **no** form of this command.

Cisco Unified Border Element

dspfarm profile *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]

no dspfarm profile *profile-identifier*

Cisco Unified Border Element (Enterprise) Cisco ASR 1000 Series Router

dspfarm profile *profile-identifier* {**transcode**}

no dspfarm profile *profile-identifier*

Cisco Integrated Services Routers Generation 2 (Cisco ISR G2)

dspfarm profile *profile-identifier* {**conference** [**video** [**homogeneous** | **heterogeneous** | **guaranteed-audio**]] | **mtp** | **transcode** [**video** | **universal**] } [**security**]

no dspfarm profile *profile-identifier*

Syntax Description

profile-identifier	Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.
conference	Enables a profile for conferencing.
mtp	Enables a profile for Media Termination Point (MTP).
transcode	Enables a profile for transcoding.
security	Enables a profile for secure DSP farm services.
video	(Optional) Enables a profile for video conferencing or transcoding.
homogeneous	(Optional) Specifies that all video participants use the one video format that is configured in this profile. DSP resources are reserved to support the conference at configuration time. **Note** The homogeneous profiles only support one video codec.
heterogeneous	(Optional) Specifies that video participants can use the different video formats that are configured in the profile. You can configure up to 10 video codecs in the heterogeneous profile. DSP resources are reserved to support the different configurations at configuration time.
guaranteed-audio	(Optional) Specifies that video participants in a heterogeneous conference will at least have an audio connection. You can configure up to 10 video codecs in the guaranteed-audio profile. The DSP resources for audio streams are reserved at configuration time, but DSP resources to support video conferences are not reserved. If the video endpoint supports the video format specified in the profile and DSP resources are available when the participant joins the conference, the participant joins as a video conferee in the video conference.

Command Default If this command is not entered, no profiles are defined for the DSP farm services.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)XW	The **security** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.0(1)M2 15.1(1)T	Support was modified for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 224 platforms.
Cisco IOS XE Release 3.2S	This command was modified. Support was added to the Cisco ASR 1000 Series Router. The **conference**, **mtp** & **security** keywords are not supported on the Cisco ASR 1000 Series Router in this release.
15.1(4)M	This command was modified. The **video** keyword was added.

Usage Guidelines Use this command to create a new profile or delete a disabled profile. After you create a new profile in dspfarm profile configuration mode, use the **no shutdown** command to enable the profile configuration, allocate resources and associate the profile with the application(s). If the profile cannot be enabled due to lack of resources, the system prompts you with a message "Can not enable the profile due to insufficient resources, resources available to support X sessions; please modify the configuration and retry."

If the DSP farm profile is successfully created, you enter the DSP farm profile configuration mode. You can configure multiple profiles for the same service.

Use the **no dspfarm profile** command to delete a profile from the system. If the profile is active, you cannot delete it; you must first disable it using the **shutdown** command. To modify a DSP farm profile, use the **shutdown** command in dspfarm profile configuration mode before you begin configuration.

The *profile identifier* uniquely identifies a profile. If the service type and *profile identifier* are not unique, the user is prompted with a message to choose a different profile identifier.

You must use the **security** keyword in order to enable secure DSP farm services such as secure transcoding.

Effective with Cisco IOS Releases 15.0(1)M2 and 15.1(1)T, platform support for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 225 is modified. These platforms are designed as TDM-IP devices and are not expandable to install extra DSP resources. So even though the **conference** keyword appears in the command syntax, this DSP service is not configurable on these platforms. If you try to configure conferencing on these platforms, the command-line interface displays the following message: "`%This platform does not support Conferencing feature.`"

The **transcode** keyword also appears in the command syntax, but this DSP service is not available on the Cisco VG 202, VG 204, and VG 224 platforms. If you try to configure transcoding on these platforms, the CLI displays the following message: "`%This platform does not support Transcoding feature.`"

Cisco ASR 1000 Series Router

The support for dspfarm profile command was added on Cisco ASR 1000 Series Router from Cisco IOS XE Release 3.2 and later releases. The command is used to create a dspfarm profile for different services.

Note The secure DSP farm services is always enabled for SPA-DSP on Cisco ASR 1000 Series Router. Only **transcode** keyword is supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s. The **conference**, **media**, and **security** keywords are not supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s.

In order to configure a video dspfarm profile, you must set **voice-service dsp-reservation** to be less than 100 percent.

To enable dspfarm profiles for voice services, you must use the **dsp services dspfarm command** under the voice-card submode.

Examples

The following example enables DSP farm services profile 20 for conferencing:

```
Router(config)# dspfarm profile 20 conference
```

Note the response if the profile is already being used:

```
Router(config)# dspfarm profile 6 conference

Profile id 6 is being used for service TRANSCODING
 please select a different profile id
```

The following example enables DSP farm services profile 1 for transcoding:

```
Router(config)# dspfarm profile 1 transcode
```

Video Conferences

The following example enables DSP farm services profile 99 for homogeneous video. The conference supports four participants under one format (Video codec H.263, qcif resolution, and a frame-rate of 15 f/s).

```
Router(config)# dspfarm profile 99 conference video homogeneous
Router(config-dspfarm-profile)# codec h263 qcif frame-rate 15
Router(config-dspfarm-profile)# maximum conference-participant 4
```

Related Commands

Command	Description
dsp service dspfarm	Configures the DSP farm services for a specified voice card.
shutdown (DSP farm profile)	Disables the DSP farm profile.
voice-card	Enters voice card configuration mode
voice-service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources. This command is required to enable video services.

dspfarm rtp timeout

To specify the Real-Time Transport Protocol (RTP) timeout interval used to clear hanging connections, use the **dspfarm rtp timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm rtp timeout *seconds*

no dspfarm rtp timeout

Syntax Description

seconds	RTP timeout interval, in seconds. Range is from 10 to 7200. Default is 1200.

Command Default

1200 seconds (20 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

Use this command to set the RTP timeout interval for when the error condition “RTP port unreachable” occurs.

Examples

The following example sets the RTP timeout value to 600 seconds (10 minutes):

```
Router# dspfarm rtp timeout 600
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm connection interval	Specifies the time interval during which to monitor RTP inactivity before deleting an RTP stream.
show dspfarm	Displays summary information about DSP resources.

dspfarm transcoder maximum sessions

To specify the maximum number of transcoding sessions to be supported by the digital-signal-processor (DSP) farm, use the **dspfarm transcoder maximum sessions** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm transcoder maximum sessions *number*

no dspfarm transcoder maximum sessions

Syntax Description

number	Number of transcoding sessions.

Command Default 0 sessions

Command Modes Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before using this command, you must disable DSP-farm service using the **no dspfarm** command.

Use this command in conjunction with the **dspfarm confbridge maximum sessions** commands.

The maximum number of transcoding sessions depends upon DSP availability in the DSP farm. A single DSP supports four transcoding sessions transmission to and from G.711 and G.729 codecs.

Examples The following example configures an NM-HDV or NM-HDV-FARM, specifies the maximum number of transcoding sessions, and enables DSP-farm services:

```
Router# configure terminal
Router(config)# no dspfarm
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
Router(config)# dspfarm transcoder maximum sessions 15
Router(config)# dspfarm
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm confbridge maximum sessions	Specifies the maximum number of conferencing sessions to be supported by a DSP farm.
dsp services dspfarm	Specifies the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled.
show dspfarm	Displays summary information about DSP resources.

dspint dspfarm

To enable the digital signal processor (DSP) interface, use the **dspint dspfarm** command in global configuration mode. This command does not have a no form.

dspint dspfarm *slot*/*port*

Syntax Description

slot	Slot number of the interface.
port	Port number of the interface.

Command Default Enabled

Command Modes Global configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(13)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines DSP mapping occurs when DSP resources on one advanced interface module (AIM) or network module are available for processing of voice time-division multiplexing (TDM) streams on a different network module or on a voice/WAN interface card (VWIC). This command is used on Cisco 3660 routers with multiservice interchange (MIX) modules installed or on Cisco 2600 series routers with AIMs installed.

To reach voice-card configuration mode for a particular voice card, from global configuration mode enter the **voice-card** command and the slot number for the AIM or network module that you want to add to the pool. See the **voice-card** command reference for details on slot numbering.

The assignment of DSP pool resources to particular TDM streams is based on the order in which the streams are configured using the **ds0-group** command for T1/E1 channel-associated signaling (CAS) or using the **pri-group** command for ISDN PRI.

The assignment of DSP pool resources does not occur dynamically during call signaling.

To disable the interface use the **no shutdown** command.

Examples The following example creates a DSP farm interface with a slot number of 1 and a port number of 0.

```
dspint dspfarm 1/0
```

To change codec complexity on the Cisco 7200 series, you must enter the following commands:

```
Router# configure terminal
Router(config)# dspint dspfarm 2/0
Router(config-dspfarm)# codec medium | high ecan-extended
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller
no shutdown	Disables the interface.
pri-group	Specifies an ISDN PRI on a channelized T1 or E1 controller
show interfaces dspfarm dsp	Displays information about the DSP interface.
voice-card	Enters voice-card configuration mode.

dtmf-interworking rtp-nte

To enable a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from Cisco Unified Border Element (Cisco UBE) or Cisco Unified Communications Manager Express (Cisco Unified CME), use the **dtmf-interworking rtp-nte** command in voice-service or dial-peer configuration mode. To remove the delay amount, use the no form of this command.

dtmf-interworking rtp-nte

no dtmf-interworking rtp-nte

Syntax Description

This command has no arguments or keywords.

Command Default

RFC 2833 packet is sent in a single burst of three dtmf-digit begin events, one duration equaling 50ms, and three dtmf-digit end events with a duration of 100ms.

Command Modes

Voice-service configuration (config-voi-serv)
Dial-peer configuration (config-dial-peer)

Command History

Cisco IOS Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If your system is configured for RFC 2833 DTMF interworking and if the remote system cannot handle RFC 2833 packets sent in a single burst, use this command to introduce a delay between the dtmf-digit begin and end events in the RFC 2833 packet.

Examples

The following example shows a delay between the dtmf-digit and events being configured.

```
Router(config-voi-serv) dtmf-interworking rtp-nte
```

Related Commands

Command	Description
nte-end-digit-delay	Specifies length of delay for each digit in dtmf-digit end event.
keypad-normalize	Ensures that the delay configured for a dtmf-end event is always honored.

dtmf timer inter-digit

To configure the dual tone multifrequency (DTMF) interdigit timer for a DS0 group, use the **dtmf timer inter-digit** command in T1 controller configuration mode. To restore the timer to its default value, use the **no** form of this command.

dtmf timer inter-digit *milliseconds*

no dtmf timer inter-digit

Syntax Description

milliseconds	DTMF interdigit timer duration, in milliseconds. Range is from 250 to 3000. The default is 3000.

Command Default 3000 milliseconds

Command Modes T1 controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.

Usage Guidelines Use the **dtmf timer inter-digit** command to specify the duration in milliseconds the router waits to detect the end of DTMF digits. After this period, the router expects no more digits to arrive and establishes the call.

Examples The following example, beginning in global configuration mode, sets the DTMF interdigit timer value to 250 milliseconds:

```
controller T1 2
 ds0-group 2 timeslots 4-10 type e&m-fgb dtmf dnis
 cas-custom 2
 dtmf timer inter-digit 250
```

Related Commands

Command	Description
cas-custom	Customizes E1 R2 signaling parameters for a particular E1 channel group on a channelized E1 line.
ds0-group	Configures channelized T1 time slots, which enables a Cisco AS5300 modem to answer and send an analog call.

dtmf-relay (Voice over Frame Relay)

To enable the generation of FRF.11 Annex A frames for a dial peer, use the **dtmf-relay** command in dial peer configuration mode. To disable the generation of FRF.11 Annex A frames and return to the default handling of dial digits, use the **no** form of this command.

dtmf-relay

no dtmf-relay

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T, and implemented on the Cisco 7200 series router.

Usage Guidelines

Cisco recommends that this command be used with low bit-rate codecs.

When **dtmf-relay** (VoFR) is enabled, the digital signal processor (DSP) generates Annex A frames instead of passing a dual-tone multifrequency (DTMF) tone through the network as a voice sample. For information about the payload format of FRF.11 Annex A frames, see the *Cisco IOS Wide-Area Networking Configuration Guide*.

Examples

The following example shows how to enable FRF.11 Annex A frames for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
 dtmf-relay
```

Related Commands

Command	Description
called-number (dial peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
connection	Specifies a connection mode for a voice port.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.

Command	Description
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

dtmf-relay (Voice over IP)

To specify how an H.323 or Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network, use the **dtmf-relay** command in dial peer voice configuration mode. To remove all signaling options and send the DTMF tones as part of the audio stream, use the **no** form of this command.

dtmf-relay {[**cisco-rtp**] [**h245-alphanumeric**] [**h245-signal**] [**rtp-nte** [**digit-drop**]] [**sip-notify**]}

no dtmf-relay

Syntax Description

cisco-rtp	Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.
h245-alphanumeric	Forwards DTMF tones by using the H.245 "alphanumeric" User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.
h245-signal	Forwards DTMF tones by using the H.245 "signal" User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.
rtp-nte	Forwards DTMF tones by using RTP with the Named Telephone Event (NTE) payload type.
digit-drop	Passes digits out-of-band and drops in-band digits are dropped. **Note** The **digit-drop** keyword is only available when the **rtp-nte** keyword is configured.
sip-notify	Forwards DTMF tones using SIP NOTIFY messages. This keyword is available only if the VoIP dial peer is configured for SIP.

Command Default

DTMF tones are disabled and sent in-band. That is, they are left in the audio stream.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco AS5300.
12.0(2)XH	The **cisco-rtp**, **h245-alphanumeric**, and **h245-signal** keywords were added.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(7)XK	This command was first supported for VoIP on the MC3810.
12.1(2)T	Changes made in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release.

Release	Modification
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(15)ZJ	The **sip-notify** keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **digit-drop** keyword was added.

Usage Guidelines

DTMF is the tone generated when you press a button on a touch-tone phone. This tone is compressed at one end of a call; when the tone is decompressed at the other end, it can become distorted, depending on the codec used. The DTMF relay feature transports DTMF tones generated after call establishment out-of-band using either a standard H.323 out-of-band method or a proprietary RTP-based mechanism. For SIP calls, the most appropriate method to transport DTMF tones is RTP-NTE or SIP-NOTIFY.

This command specifies how an H.323 or SIP gateway relays DTMF tones between telephony interfaces and an IP network.

You must include one or more keywords when using this command.

To avoid sending both in-band and out-of band tones to the outgoing leg when sending IP-to-IP gateway calls in-band (rtp-nte) to out-of band (h245-alphanumeric), configure the **dtmf-relay** command using the **rtp-nte** and **digit-drop** keywords on the incoming SIP dial peer. On the H.323 side, and for H.323 to SIP calls, configure this command using either the **h245-alphanumeric** or **h245-signal** keyword.

The SIP-NOTIFY method sends NOTIFY messages bidirectionally between the originating and terminating gateways for a DTMF event during a call. If multiple DTMF relay mechanisms are enabled on a SIP dial peer and are negotiated successfully, the SIP-NOTIFY method takes precedence.

SIP NOTIFY messages are advertised in an invite message to the remote end only if the **dtmf-relay** command is set.

For SIP, the gateway chooses the format according to the following priority:

1. sip-notify (highest priority)
2. rtp-nte
3. None—DTMF sent in-band

The gateway sends DTMF tones only in the format that you specify if the remote device supports it. If the H.323 remote device supports multiple formats, the gateway chooses the format according to the following priority:

1. cisco-rtp (highest priority)
2. h245-signal
3. h245-alphanumeric
4. rtp-nte
5. None—DTMF sent in-band

The principal advantage of the **dtmf-relay** command is that it sends DTMF tones with greater fidelity than is possible in-band for most low-bandwidth codecs, such as G.729 and G.723. Without the use of DTMF relay, calls established with low-bandwidth codecs may have trouble accessing automated DTMF-based systems, such as voice mail, menu-based Automatic Call Distributor (ACD) systems, and automated banking systems.

Note

- The **cisco-rtp** keyword supports a proprietary Cisco implementation and operates only between two Cisco 2600 series or Cisco 3600 series routers running Cisco IOS Release 12.0(2)XH or later. Otherwise, the DTMF relay feature does not function, and the gateway sends DTMF tones in-band.
- The **cisco-rtp** keyword is supported on Cisco 7200 series routers.
- The **sip-notify** keyword is available only if the VoIP dial peer is configured for SIP.
- The **digit-drop** keyword is available only when the **rtp-nte** keyword is configured.

Examples

The following example configures DTMF relay with the **cisco-rtp** keyword when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp
```

The following example configures DTMF relay with the **cisco-rtp** and **h245-signal** keywords when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp h245-signal
```

The following example configures the gateway to send DTMF in-band (the default) when DTMF tones to are sent dial peer 103:

```
dial-peer voice 103 voip
 no dtmf-relay
```

The following example configures DTMF relay with the **digit-drop** keyword to avoid both in-band and out-of band tones being sent to the outgoing leg on H.323 to H.323 or H.323 to SIP calls:

```
dial-peer voice 1 voip
 session protocol sipv2
 dtmf-relay h245-alphanumeric rtp-nte digit-drop
```

The following example configures DTMF relay with the **rtp-nte** keyword when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay rtp-nte
```

The following example configures the gateway to send DTMF tones using SIP NOTIFY messages to dial peer 103:

```
dial-peer voice 103 voip
 session protocol sipv2
 dtmf-relay sip-notify
```

Related Commands

Command	Description
notify telephone-event	Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.

dualtone

To enter cp-dualtone configuration mode for specifying a custom call-progress tone, use the **dualtone** command in custom-cptone voice-class configuration mode. To configure the custom-cptone voice class not to detect a call-progress tone, use the **no** form of this command.

dualtone {**busy** | **conference** | **disconnect** | **number-unobtainable** | **out-of-service** | **reorder** | **ringback**}

no dualtone {**busy** | **conference** | **disconnect** | **number-unobtainable** | **out-of-service** | **reorder** | **ringback**}

Syntax Description

busy	Configure busy tone.
conference	Configure conference join and leave tones.
disconnect	Configure disconnect tone.
number-unobtainable	Configure number-unavailable tone.
out-of-service	Configure out-of-service tone.
reorder	Configure reorder tone.
ringback	Configure ringback tone.

Command Default

No call-progress tones are defined within the custom-cptone voice class

Command Modes

Custom-cptone voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 and Cisco 3600 series and on the Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750 router and integrated into Cisco IOS Release 12.2(2)T.
12.4(11)XJ2	The **conference** keyword was added.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **dualtone** command enters cp-dualtone configuration mode and specifies a call-progress tone to be detected. You can specify additional call-progress tones without exiting cp-dualtone configuration mode.

Any call-progress tones that are not specified are not detected.

To delete a call-progress tone from this custom-cptone voice class, use the **no** form of this command and the keyword for the tone that should not be detected; for example, **no dualtone busy**.

You must associate the class of custom call-progress tones with a voice port for this command to affect tone detection.

Use the **dualtone conference** command to define custom join and leave tones for hardware conferences.

Examples

The following example enters cp-dualtone configuration mode and specifies busy tone and ringback tone in the custom-cptone voice class country-x.

```
Router(config)# voice class custom-cptone country-x
Router(cfg-cptone)# dualtone busy
Router(cfg-cp-dualtone)# frequency 440 480
Router(cfg-cp-dualtone)# cadence 500 500
Router(cfg-cp-dualtone)# exit
Router(cfg-cptone)# dualtone ringback
Router(cfg-cp-dualtone)# frequency 400 440
Router(cfg-cp-dualtone)# cadence 2000 4000
```

The following example deletes ringback tone from the custom-cptone voice class country-x.

```
Router(config)# voice class custom-cptone country-x
Router(cfg-cptone)# no dualtone ringback
```

The following example configures a conference leave tone. The configured leave tone must be associated with a digital signal processor (DSP) farm profile.

```
Router(config)# voice class custom-cptone leavetone
Router(cfg-cptone)# dualtone conference
Router(cfg-cp-dualtone)# frequency 500 500
Router(cfg-cp-dualtone)# cadence 100 100 100 100 100
```

Related Commands

Command	Description
cadence	Defines the tone on and off durations for a call-progress tone.
conference-join custom-cptone	Defines a custom call-progress tone to indicate joining a conference.
conference-leave custom-cptone	Defines a custom call-progress tone to indicate leaving a conference.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
frequency	Defines the frequency components for a call-progress tone.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

Cisco IOS Voice Commands: E

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

e911

To enable E911 system services for SIP on the VoIP dial peer, use the **e911** command in voice service VoIP configuration mode. To disable SIP E911 functionality, use the **no** form of this command.

e911

no e911

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Voice service VoIP (dial peer) configuration mode.

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **no** form of the command disables E911 functionality from a global perspective. Output from the **show running-config** command shows whether E911 is configured. See also the **voice-class sip e911** and **debug csm neat** commands.

Examples

The following example enables E911 services in voice service VoIP SIP configuration mode:

```
Router# configure terminal
Router(config-term)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# e911
```

The following example disables E911 functionality:

```
Router(conf-serv-sip)# no e911
```

Related Commands

Command	Description
debug csm neat	Turns on debugging for all Call Switching Module (CSM) Voice over IP (VoIP) calls.
show running-config	Displays the current configuration information.
voice-class sip e911	Configures e911 services on the voice dial peer.

early-offer

To force a Cisco Unified Border Element (Cisco UBE) to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL), use the **early-offer** command in SIP or dial peer configuration mode. To disable Early-Offer, use the **no** form of this command.

early-offer forced

no early-offer forced

Syntax Description

forced	Forcefully sends Early-Offer on the SIP Out-Leg.

Command Default

Disabled. The Cisco UBE does not distinguish SIP Delayed-Offer to Early-Offer call flows.

Command Modes

SIP configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to forcefully configure a Cisco UBE to send a SIP invite with EO on the Out-Leg (OL), Delayed-Offer to Early-Offer for all VoIP calls, SIP audio calls, or individual dial peers.

Examples

The following example shows SIP Early-Offer invites being configured globally:

```
Router(conf-serv-sip)# early-offer forced
```

The following example shows SIP Early-Offer invites being configured per dial peer:

```
Router(config-dial-peer)# voice-class sip early-offer forced
```

echo-cancel comfort-noise

To specify that background noise be generated, use the **echo-cancel comfort-noise** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel comfort-noise

no echo-cancel comfort-noise

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines Use the **echo-cancel comfort-noise** command to generate background noise to fill silent gaps during calls if voice activated dialing (VAD) is activated. If comfort noise is not enabled and VAD is enabled at the remote end of the connection, the user hears nothing or silence when the remote party is not speaking.

The configuration of comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples The following example enables comfort noise on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel comfort-noise
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.
voice port	Specifies which port is used for voice traffic.

echo-cancel compensation

To set attenuation for loud signals, use the **echo-cancel compensation** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel compensation

no echo-cancel compensation

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines Use the **echo-cancel compensation** command to add attenuation control to the T1 or E1 controller. When this command is enabled, 6 decibels of attenuation are inserted if the signal level from the receive direction is loud. When loud signals are not received, the attenuation is removed.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples The following example enables attenuation control on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel compensation
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.
voice port	Specifies which port is used for voice traffic.

echo-cancel coverage

To adjust the size of the echo canceller (EC) and to select the extended EC when the Cisco default EC is present, use the **echo-cancel coverage** command in voice-port configuration mode. To reset this command to the default value (64 ms), use the **no** form of this command.

echo-cancel coverage {**8** | **16** | **24** | **32** | **48** | **64**}

no echo-cancel coverage

Syntax Description

8	EC size of 8 ms.
16	EC size of 16 ms.
24	EC size of 24 ms.
32	EC size of 32 ms.
48	EC size of 48 ms.
64	EC size of 64 ms. This is the default.

Command Default 64 ms

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(5)XK	The command was modified to add the 8-ms option.
12.0(5)XE	The command was implemented on the Cisco 7200 series.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(13)T	This command was modified to provide a new set of size options when the extended EC is configured. This command is supported on all T1 Digital Signal Processor (DSP) platforms.
12.3(11)T	This command was modified for use on NextPort platforms for use with the dual-filter G.168 echo canceller.

Usage Guidelines Use the **echo-cancel coverage** command to adjust the coverage size of the EC. This command enables cancellation of voice that is sent out the interface and received on the same interface within the configured amount of time. If the local loop (the distance from the interface to the connected equipment that is producing the echo) is greater than this amount of time, the configured value of this command should be increased.

If you configure a greater value for this command, the EC takes longer to converge. In this case, you might hear a slight echo when the connection is initially set up. If the configured value for this command is too short, you might hear some echo for the duration of the call because the EC is not canceling the longer delay echoes.

There is no echo or echo cancellation on the network side (for example, the non-POTS side) of the connection.

Note This command is valid only if the echo cancellation feature has been enabled. For more information, see the **echo-cancel enable** command.

The NextPort dual-filter G.168 echo canceller feature supports echo tails from 8 to 64 ms in 8-ms increments. Use the **echo-cancel coverage** command to limit the echo canceller coverage to 64 ms on NextPort platforms. Tail length values greater than 64 ms are not accepted with the NextPort dual-filter G.168 echo canceller feature. For more information about the NextPort dual0filter G.168 echo canceller, see *NextPort Voice Tuning and Background Noise Statistics with NextPort Dual-Filter G.168 Echo Cancellation*.

Examples

The following example enables the extended echo cancellation feature and adjusts the size of the echo canceller to 16 milliseconds:

```
Router (config-voiceport)# echo-cancel coverage 16
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a controller.
echo-cancel enable	Enables echo cancellation on a voice port.

echo-cancel enable

To enable the cancellation of voice that is sent out the interface and received back on the same interface, use the **echo-cancel enable** command in voice-port configuration mode or global configuration mode. To disable echo cancellation, use the **no** form of this command.

echo-cancel enable type [**hardware** | **software**]

no echo-cancel enable

Syntax Description

hardware	(Optional) Specifies that echo cancellation is enabled via the hardware on the network module.
software	(Optional) Specifies that echo cancellation is enabled via command-line interface entries.

Note The **hardware** and **software** keywords are available only when the optional hardware echo cancellation module is installed on the multiflex VWIC.

Command Default

The Cisco-proprietary G.168 echo canceller (EC) is enabled with the echo suppressor turned off.

Command Modes

Voice-port configuration
Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command is supported on all TI Digital Signal Processor (DSP) platforms.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T and the optional **hardware** and **software** keywords were added.

Usage Guidelines

The **echo-cancel enable** command enables cancellation of voice that is sent out the interface and received back on the same interface; sound that is received back in this manner is perceived by the listener as an echo. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

Typically a hybrid circuit can provide greater than 6 decibels (dB) echo return loss (ERL), so the extended EC is configured to handle 6 dB worst case by default. However, if a measurement shows that a circuit can provide only 6 dB ERL or less, the extended EC can be configured to use this lower rate.

The Cisco G.168 EC is enabled by default with the echo suppressor turned off. The echo suppressor can be turned on only when the default Cisco G.168 EC is used. The **echo-cancel suppressor** command used with the Cisco default EC is still visible when the extended EC is selected, but it does not do anything.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.

There is no echo path for a 4-wire recEive and transMit interface (also called ear and mouth and abbreviated as E&M). The echo canceller should be disabled for that interface type.

Note This command is valid only when the **echo-cancel coverage** command has been configured.

Examples

The following example enables the extended echo cancellation feature in voice-port configuration mode:

```
Router (config-voiceport)# echo-cancel enable
```

The following example enables the extended echo cancellation feature on the Cisco 1700 series or Cisco ICS7750 in global configuration mode:

```
Router (config)# echo-cancel enable
```

Related Commands

Command	Description
echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
echo-cancel enable (controller)	Enables echo cancellation on a controller.
echo-cancel suppressor	Enables echo suppression to reduce initial echo before the echo canceller converges.
non-linear	Enables nonlinear processing in the echo canceler.

echo-cancel enable (controller)

To enable the echo cancel feature, use the **echo-cancel enable** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel enable

no echo-cancel enable

Syntax Description This command has no arguments or keywords.

Command Default Enabled for all interface types

Command Modes Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines The **echo-cancel enable** command enables cancellation of voice that is sent out of the interface and received back on the same interface. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.

Note This command is valid only if the **echo-cancel coverage** command has been configured.

The following example enables the echo cancel feature on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
```

Related Commands

Command	Description
echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
echo-cancel enable	Enables echo cancellation on a voice port.
non-linear	Enables nonlinear processing in the echo canceler.
voice port	Configures the voice port.

echo-cancel erl worst-case

To determine worst-case Echo Return Loss (ERL) in decibels (dB), use the **echo-cancel erl worst-case** command in voice-port configuration mode. To disable the command, use the **no** form.

echo-cancel erl worst-case {**6** | **3** | **0**}

no echo-cancel erl worst-case {**6** | **3** | **0**}

Syntax Description

6 | **3** | **0**	Values of 6, 3, or 0 dB ERL in the extended echo canceller (EC). The default is 6.

Command Default Enabled at 6 dB when the extended G.168 EC is used

Command Modes Voice-port configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines This command is used only when the extended EC is present and is not supported with the Cisco proprietary-G.165 EC. This command predicts the worst-case ERL that the EC might encounter.

Examples The following example shows a worst-case ERL of 3:

```
Router(config-voiceport)# echo-cancel erl worst-case 3
```

To check the configuration, enter the **show voice port** command in privileged EXEC mode:

```
Router# show voice port
.
.
Echo Cancel worst case ERL is set to 6 dB
Playout-delay Mode is set to adaptive
.
.
```

Related Commands

Command	Description
echo-cancel enable	Enables the cancellation of voice that is sent out and received on the same interface.

echo-cancel loopback

To place the echo cancellation processor in loopback mode, use the **echo-cancel loopback** command in controller configuration mode. To disable loopback of the echo cancellation processor, use the **no** form of this command.

echo-cancel loopback

no echo-cancel loopback

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Controller configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines Use an **echo-cancel loopback** test on lines to detect and distinguish equipment malfunctions caused by either the line or the interface. If correct echo cancellation is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples The following example sets up echo cancellation loopback diagnostics:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
 echo-cancel loopback
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a controller.

echo-cancel mode

To enable echo cancel mode on the extended G.168 echo canceller, use the **echo-cancel mode** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

echo-cancel mode {**1** | **2**}

no echo-cancel mode

Syntax Description

1	Enables fast convergence for multiple echo reflectors and applies 0 dB Sin gain and 0 dB Sout gain.
2	Enables fast convergence for multiple echo reflectors and improves double-talk detection by applying 6 dB Sin gain and -6 dB Sout gain.

Command Default Disabled

Command Modes Voice-port configuration

Command History

Release	Modification
12.3(7)	This command was introduced.

Usage Guidelines This command enables an operation mode to improve echo canceller (EC) performance in systems that have multiple echo reflectors and double-talk caused by low volume. When this command is enabled, the extended EC cancels the echo better in multiple echo reflector scenarios, which occur most often in analog interfaces.

Note

- This command is available only if the extended G.168 echo canceller is enabled for the voice port.
- If you select mode **2**, set the **echo-cancel erl worst-case** command to 0.

Examples The following example sets the extended G.168 EC mode to 1 on a Cisco 1700 series router:

```
Router(config)# voice-port 1/0/1
Router(config-voiceport)# echo-cancel mode 1
```

Related Commands

Command	Description
echo-cancel coverage	Adjusts the size of the echo canceller.
echo-cancel enable	Enables echo cancellation for voice that is sent and received on the same interface.
echo-cancel erl worst-case	Determines worst-case Echo Return Loss (ERL).

echo-cancel suppressor

To enable echo suppression to reduce initial echo before the echo canceller converges, use the **echo-cancel suppressor** command in voice-port configuration mode. To disable echo suppression, use the **no** form of this command.

echo-cancel s uppressor *seconds*

no echo-cancel suppressor

Syntax Description

seconds	Suppressor coverage, in seconds. Range is from 1 to 10. Default is 7.

Command Default Disabled

Command Modes Voice-port configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines This command is used only when the echo canceller is enabled. In case of double-talk in the first number of seconds, the code automatically disables the suppressor.

Examples The following example shows echo suppression configured for a suppression coverage of 9 seconds:

```
Router(config-voiceport)# echo-cancel suppressor 9
```

Related Commands

Command	Description
echo-cancel enable	Enables the cancellation of voice that is sent out and received on the same interface.

element

To define component elements of local or remote clusters, use the **element** command in gatekeeper configuration mode. To disable component elements of local or remote clusters, use the **no** form of this command.

element *gatekeeper-name ip-address* [*port*]

no element *gatekeeper-name ip-address* [*port*]

Syntax Description

gatekeeper-name	Name of the gatekeeper component to be added to the local or remote cluster.
ip-address	IP address of the gatekeeper to be added to the local or remote cluster.
port	(Optional) Registration, Admission, and Status (RAS) signaling port number for the remote zone. Range is from 1 to 65535. Default is the well-known RAS port number 1719.

Command Default No default behavior or values

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Examples The following example places the GenevaGK gatekeeper into the specified local or remote cluster:

```
element GenevaGK 172.16.204.158 1719
```

Related Commands

Command	Description
zone cluster local	Defines a local grouping of gatekeepers, including the gatekeeper that you are configuring.
zone cluster remote	Defines a remote grouping of gatekeepers, including the gatekeeper that you are configuring.

emptycapability

To eliminate the need for identical codec capabilities for all dial peers in the rotary group, use the **emptycapability** command in h.323 voice-service configuration mode. To return to the default configuration, use the **no** form of this command.

emptycapability

no emptycapability

Syntax Description

There are no keywords or arguments for this command.

Command Default

Identical codec capabilities are required on all dial peers.

Command Modes

H.323 voice-service configuration mode

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The default dial-peer configuration requires that all members of a hunt group must have the same codec configured to complete calls. Configuring **emptycapability** on the IP-to-IP gateway (IPIPGW) eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the IPIPGW to restart the codec negotiation end-to-end.

Note If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

Examples

The following example shows emptycapability being configured to allow the IPIPGW to restart codec negotiation from end-to-end regardless of codec configured on each endpoint:

```
Router(conf-serv-h323)# emptycapability
```

Related Commands

Command	Description
h323	Enters H.323 voice service configuration mode.

emulate cisco h323 bandwidth

To instruct the H.323 gateway to use H.323 version 2 behavior for bandwidth management, use the **emulate cisco h323 bandwidth** command in gateway configuration mode. To instruct the gateway to use H.323 version 3 behavior for bandwidth management, use the **no** form of the command.

emulate cisco h323 bandwidth

no emulate cisco h323 bandwidth

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviors or values

Command Modes

Gateway configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Prior to Cisco IOS Release 12.2(2)XA, gateway calls were always reported to require a bandwidth of 64 kbps, the unidirectional bandwidth for a Cisco G.711 codec. If the endpoints in the call chose to use a more efficient codec, this was not reported to the Cisco gatekeeper.

In the version of the Cisco H.323 gateway in Cisco IOS Release 12.2(2)XA or later (which conforms with H.323 version 3), the reported bandwidth is bidirectional. Initially, 128 kbps is reserved. If the endpoints in the call select a more efficient codec, the Cisco gatekeeper is notified of the bandwidth change.

For backward compatibility, the **emulate cisco h323 bandwidth** command allows devices running Cisco IOS Release 12.2(2)XA and later to conform to the H.323 version 2 bandwidth reporting implementation.

Examples

The following example shows that the router emulates the behavior of a Cisco H.323 Version 2 gateway.

```
Router(config-gateway)# emulate cisco h323 bandwidth
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
gateway	Enables gateway configuration commands.

encap clear-channel standard

To globally enable RFC 4040-based clear-channel codec negotiation for Session Initiation Protocol (SIP) calls on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE), use the **encap clear-channel standard** command in voice service SIP configuration mode. To disable RFC 4040-based clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE, use the **no** form of this command.

encap clear-channel standard

no encap clear-channel standard

Syntax Description

standard	Specifies standard RFC 4040 encapsulation.

Command Default

Disabled—legacy encapsulation [X-CCD/8000] is used for clear-channel codec negotiation.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **encap clear-channel standard** command in voice service SIP configuration mode to globally enable RFC 4040-based clear-channel codec negotiation [CLEARMODE/8000] for SIP calls on a Cisco IOS voice gateway or Cisco UBE. RFC 4040-based clear-channel codec negotiation allows Cisco IOS voice gateways and Cisco UBEs to successfully interoperate with third-party SIP gateways that do not support legacy Cisco IOS clear-channel codec encapsulation [X-CCD/8000].

When the **encap clear-channel standard** command is enabled on a Cisco IOS voice gateway or Cisco UBE, calls using the Cisco IOS clear channel codec are translated into calls that use CLEARMODE/8000 so that the calls do not get rejected when they reach third-party SIP gateways.

To enable RFC 4040-based clear-channel codec negotiation for SIP calls on an individual dial peer, overriding the global configuration for the Cisco IOS voice gateway or Cisco UBE, use the **voice-class sip encap clear-channel standard** command in dial peer voice configuration mode. To globally disable RFC 4040-based clear-channel codec negotiation on a Cisco IOS voice gateway or Cisco UBE, use the **no encap clear-channel standard** command in voice service SIP configuration mode.

Examples

The following example shows how to enable RFC 4040-based clear-channel code negotiation globally for all dial peers on a Cisco IOS voice gateway or Cisco UBE:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# encap clear-channel standard
```

Related Commands

Command	Description
voice-class sip encap clear-channel	Enables RFC 4040-based clear-channel codec negotiation for SIP calls on an individual dial peer on a Cisco IOS voice gateway or Cisco UBE.

encapsulation atm-ces

To enable circuit emulation service (CES) ATM encapsulation, use the **encapsulation atm-ces** command in interface configuration mode. To disable CES ATM encapsulation, use the **no** form of this command.

encapsulation atm-ces

no encapsulation atm-ces

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Interface configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0	This command was integrated into Cisco IOS Release 12.0.

Usage Guidelines This command is supported only on serial ports 0 and 1.

Examples The following example enables CES ATM encapsulation on serial port 0:

```
interface serial 0
 encapsulation atm-ces
```

Related Commands

Command	Description
ces cell-loss-integration-period	Sets the CES cell-loss integration period.
ces clockmode synchronous	Configures the ATM CES synchronous clock mode.
ces connect	Maps the CES service to an ATM PVC.
ces initial-delay	Configures the size of the receive buffer of a CES circuit.
ces max-buf-size	Configures the send buffer of a CES circuit.
ces partial-fill	Configures the number of user octets per cell for the ATM CES.
ces service	Configures the ATM CES type.

encoding h450 call-identity

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

encoding h450 call-identity{**cisco** | **itu**}

no encoding h450 call-identity

Syntax Description

cisco	Gateway uses a PER encoding format that is not compliant with ITU X.691 for encoding or decoding the H.450.2 callIdentity field.
itu	Gateway uses a PER encoding format that is compliant with ITU X.691 for encoding or decoding the H.450.2 callIdentity field.

Command Default Cisco encoding is enabled at the global (voice-service configuration) level.

Command Modes Voice-class configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.3(7)T3	This command was integrated into Cisco IOS release 12.3(7)T3.

Usage Guidelines Use this command to set the encoding format in the voice-class assigned to individual dial peers. By default, Cisco encoding is enabled globally. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU X.691 and can cause interoperability problems with third-party devices during H.450.2 call transfer with consultation. Use the **itu** keyword to configure ITU X.691 encoding in the dial peer.

Note This command takes precedence over the **encoding h450 call-identity itu** command in voice-service configuration mode.

Examples The following example enables X.691-compliant encoding for the H.450-2 PDUs for calls on dial-peer 4:

```
voice class h323 1
 encoding h450 call-identity itu

dial-peer voice 4 voip
 voice-class h323 1
```

The following example enables Cisco encoding, which is not compliant with ITU X.691, on dial-peer 5:

```
voice class h323 1
 encoding h450 call-identity cisco

dial-peer voice 5 voip
 voice-class h323 1
```

By entering the **no encoding h450 call-identity** command under the voice-class configuration mode, the following example sets the encoding for calls only on dial-peer 7 to reset to the global configuration. However, the **no encoding h450 call-identity** configuration is not displayed in the running configuration:

```
voice class h323 1
 no encoding h450 call-identity

dial-peer voice 7 voip
 voice-class h323 1
```

The following example illustrates a typical use case when the ITU encoding is configured for all the dial peers except dial-peer 4; dial-peer 4 uses Cisco encoding:

```
voice service voip
 h323
  encoding h450 call-identity itu

voice class h323 1
   encoding h450 call-identity cisco

dial-peer voice 1 voip
 destination-pattern 1..

dial-peer voice 2 voip
 destination-pattern 2..

dial-peer voice 3 voip
 destination-pattern 3..

dial-peer voice 4 voip
 destination-pattern 4..
 voice-class h323 1
```

Related Commands

Command	Description
encoding h450 call-identity itu	Sets the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs).
voice class h323	Enters voice-class configuration mode and creates a voice class for H.323 attributes.

encoding h450 call-identity itu

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity itu** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

encoding h450 call-identity itu

no encoding h450 call-identity

Syntax Description

This command has no argument or keywords.

Command Default

Cisco encoding enabled globally

Command Modes

Voice-service configuration

Command History

Release	Modification
12.3(11)T	This command was introduced on Cisco voice gateways.
12.3(7)T3	This command was integrated into Cisco IOS release 12.3(7)T3.

Usage Guidelines

Use this command to set ITU X.691 encoding globally on the Cisco voice gateway. By default, Cisco encoding is enabled. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU X.691 and could cause interoperability problems with third-party devices during H.450.2 call transfer with consultation.

Note The **encoding h450 call-identity** command in voice-class configuration mode takes precedence over this command.

Examples

The following example globally configures all dial-peers with the ITU X.691:

```
voice service voip
 h323
 encoding h450 call-identity itu
```

Related Commands

Command	Description
encoding h45 call-identity	Sets the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs).
voice service voip	Enters voice-service configuration mode.

encryption

To set the algorithm to be negotiated with the provider, use the **encryption** command in settlement configuration mode. To reset to the default encryption method, use the **no** form of this command.

encryption {**des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all**}

no encryption {**des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all**}

Syntax Description

des-cbc-sha	Encryption type ssl_rsa_with_des_cbc_sha cipher suite.
des40-cbc-sha	Encryption type ssl_rsa_export_with_des40_cbc_sha cipher suite.
dh-des-cbc-sha	Encryption type ssl_dh_rsa_with_des_cbc_sha cipher suite.
dh-des40-cbc-sha	Encryption type ssl_dh_rsa_export_with_des40_cbc_sha cipher suite.
null-md5	Encryption type ssl_rsa_with_null_md5 cipher suite.
null-sha	Encryption type ssl_rsa_with_null_sha cipher suite.
all	All encryption methods are used in the Secure Socket Layer (SSL).

Command Default

The default encryption method is **all**. If none of the encryption methods is configured, the system uses all of the encryption methods in the SSL session negotiation.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

For Cisco IOS Release 12.0(4)XH1, only one encryption method is allowed for each provider.

Examples

The following example sets the algorithm to be negotiated with the provider, using the **encryption** command:

```
settlement 0
     encryption des-cbc-sha
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.

Command	Description
device-id	Sets the device identification.
max-connection	Sets the maximum number of simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Disables the settlement provider.
type	Specifies the provider type.
url	Specifies the ISP address.

endpoint alt-ep collect

To configure the collection of alternate routes to endpoints, use the **endpoint alt-ep collect** command in gatekeeper configuration mode. To disable alternate route collection, use the **no** form of this command.

endpoint alt-ep collect *value* [**distribute**]

no endpoint alt-ep collect

Syntax Description

value	Number of alternate routes to endpoints for the gatekeeper to collect before ending the collection process and sending the Location Confirmation (LCF) message to the requesting endpoint. Range for the *value* argument is from 1 to 20. The default is 0, which indicates that alternate route collection is not enabled.
distribute	(Optional) Causes the gatekeeper to include alternate routes from as many LCF messages as possible in the consolidated list. Use of this keyword allows the gatekeeper to give fairness to the information of alternate routes present in various LCF messages. **Note** Identical alternate endpoints are removed from the list. That is, if an alternate endpoint received in an LCF message has an identical IP address or trunk group label or carrier ID as any alternate endpoints received in previous LCF messages, the previous duplicate alternate endpoints are removed from the consolidated list.

Command Default

The default value for the *value* argument is 0, which indicates that alternate route collection is not enabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	Duplicate alternate endpoints received in an LCF message were removed from the consolidated list of endpoints. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to force the gatekeeper to collect a specified number of alternate routes to endpoints and to create a consolidated list of those alternate routes to report back to the requesting endpoint.

Examples

The following example shows that 15 alternate routes to endpoints should be collected:

```
Router(config-gk)# endpoint alt-ep collect 15
```

Related Commands

Command	Description
endpoint alt-ep h323id	Configures an alternate endpoint on a gatekeeper, including endpoint ID, IP address, port, and trunk group label or carrier-ID information.
show gatekeeper endpoints alternates	Displays information about alternate endpoints.

endpoint alt-ep h323id

To configure alternate endpoints, use the **endpoint alt-ep h323id command in** gatekeeper configuration mode. To disable alternate endpoints, use the **no** form of this command.

endpoint alt-ep h323id *h323-id ip-address* [*port-number*] [**carrier-id** *carrier-name*]

no endpoint alt-ep h323id

Syntax Description

h323-id	H.323 name (ID) of the endpoint for which an alternate address is being supplied. This ID is used by a gateway when the gateway communicates with the gatekeeper. Usually, this H.323 ID is the name given to the gateway, with the gatekeeper domain name appended to the end.
ip-address	IP address of an alternate for this endpoint.
port-number	(Optional) Port number associated with the address of the alternate. Default is 1720.
carrier-id *carrier-name*	(Optional) Trunk group label or carrier ID of the alternate endpoint. It may be added in addition to the IP address of the alternate endpoint. The *carrier-name* argument is the name of the trunk group label or circuit ID.

Command Default

The default port number is 1720.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and the **carrier-id** keyword and *carrier-name* argument were added.

Usage Guidelines

This command defines the IP address for an alternate endpoint for the primary endpoint identified by its H.323 ID. The IP address is returned in the alternate endpoint field whenever the primary endpoint is returned in an Admission Confirmation (ACF) or Location Confirmation (LCF) message. The alternate endpoint provides an alternate address to which a call can be placed if a call to the primary endpoint fails.

This command provides a failover mechanism if a gateway becomes disabled for a period of time before the gatekeeper becomes aware of the problem. After receiving an ACF message from the gatekeeper with an alternate endpoint list, the Cisco gateway may attempt to use an alternate address if a SETUP message results in no reply from the destination. This command causes the alternate endpoints specified in the *h323-id* argument to be sent in all subsequent ACF and LCF messages. Gatekeepers that support the **endpoint alt-ep h323id** command can also send alternate endpoint information in Registration, Admissions, and Status (RAS) messages. The gatekeeper accepts IP, port call signal address, and trunk

group ID and carrier ID information in endpoint Registration Request (RRQ) messages. The gatekeeper list of alternates for a given endpoint includes the configured alternates and the alternates received in RRQ messages from that endpoint and any alternate endpoints received in incoming RAS LCF messages.

Examples

The following example shows that the endpoint at 172.16.53.15 1719 has been configured as an alternate for "GW10". There are no carrier IDs:

```
endpoint alt-ep h323id GW10 172.16.53.15 1719
```

The following example shows that an alternate endpoint list with different carrier IDs (CARRIER_ABC, CARRIER_DEF, and CARRIER_GHI) has been configured for "gwid":

```
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_ABC
endpoint alt-ep h323id gwid 2.2.2.2 carrier-id CARRIER_DEF
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_GHI
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays information about alternate endpoints.

endpoint circuit-id h323id

To associate a circuit with a non-Cisco endpoint or on using a Cisco IOS Release older than that on the gatekeeper, use the **endpoint circuit-id h323id** command in gatekeeper configuration mode. To delete the association, use the **no** form of this command.

endpoint circuit-id h323id *endpoint-h323id circuit-id* [**max-calls** *number*]

no endpoint circuit-id h323id *endpoint-h323id descriptor* [**max-calls** *number*]

Syntax Description

endpoint-h323id	ID of the H.323 endpoint.
circuit-id	Circuit assigned to the H.323 endpoint.
max-calls *number*	(Optional) Maximum number of calls that this endpoint can handle. Range is from 1 to 10000. There is no default.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **endpoint circuit-id h323id** command allows the gatekeeper and GKTMP server application to work with Cisco gateways that are running non-Cisco gateways or Cisco IOS versions that cannot identify incoming circuits. This command permits only one circuit to be associated with the endpoint.

Examples

The following example associates a non-Cisco endpoint **first** with a circuit **westcoast**, and assigns a maximum of 2750 calls to the endpoint:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint circuit-id h323-id first westcoast maxcalls 2750
```

Related Commands

Command	Description
show gatekeeper endpoint circuits	Displays information about all registered endpoints for a gatekeeper.

endpoint max-calls h323id

To set the maximum number of calls that are allowed for an endpoint, use the **endpoint max-calls h323id** command in gatekeeper configuration mode. To disable the set number, use the **no** form of this command.

endpoint max-calls h323id *endpoint-h323id max-number*

no endpoint max-calls h323id

Syntax Description

endpoint-h323id	H.323 ID of the endpoint.
max-number	Maximum number of calls that the endpoint can handle. The range is from 1 to 100000.

Command Default

This command is not configured by default.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modifications
12.3(1)	This command was introduced.
12.3(10)	This command was modified to reject the limit set by the endpoints.
12.3(14)T	This command was modified to reject the limit set by the endpoints.

Usage Guidelines

You must use the **endpoint resource-threshold** command and the **arq reject-resource-low** command to start resource monitoring on a gatekeeper before you can use this command. The **endpoint resource-threshold** command sets the call-capacity threshold of a gateway in the gatekeeper. The **arq reject-resource-low** command allows the endpoint to reject the limit of automatic repeat request message-packet (ARQs) when the endpoint reaches its configured maximum number of calls.

Examples

The following example shows how to set the maximum number of calls that GW-1 can handle to 1000:

```
gatekeeper
 endpoint max-calls h323id GW-1 1000
```

Related Commands

Command	Description
arq reject-resource-low	Enables the gatekeeper to send an ARQ to the requesting gateway if destination resources are low.
endpoint resource-threshold	Sets the call capacity threshold of a gateway in the gatekeeper.

endpoint naming

To customize the T3 endpoint naming convention on a per-MGCP-profile basis, use the **endpoint naming** command in MGCP profile configuration mode. To disable endpoint naming, use the **no** form of this command.

endpoint naming {**t1** | **t3**}

no endpoint naming

Syntax Description

t1	Flat-T3-endpoint naming convention.
t3	Hierarchical-T3-endpoint naming convention.

Command Default t1

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines The option to select between a flat-endpoint naming convention and a hierarchical-T3-endpoint naming convention gives call agents flexibility without enforcing one naming convention. Signaling, backhauling, and trunks using SS7 are supported. T3 naming conventions on XCC signaling types, SS7, and ISDN are not supported.

Examples The following example shows the T3 endpoint naming convention on an MGCP profile:

```
Router# configure terminal
Router(config)# mgcp profile default
Router(config-mgcp-profile)# endpoint naming t3
Router(config-mgcp-profile)# end
```

Related Commands

Command	Description
show mgcp	Displays MGCP configuration information.

endpoint resource-threshold

To set a gateway's call capacity thresholds in the gatekeeper, use the **endpoint resource threshold** command in gatekeeper configuration mode. To delete the thresholds, use the **no** form of this command.

endpoint resource-threshold [**onset** *high-water-mark* | **abatement** *low-water-mark*]

no endpoint resource-threshold [**onset** *high-water-mark*] [**abatement** *low-water-mark*]

Syntax Description

onset *high-water-mark*	(Optional) Maximum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 90.
abatement *low-water-mark*	(Optional) Minimum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 70.

Command Default

High-water-mark: 90 percent
Low-water-mark: 70 percent

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The gatekeeper monitors the call volume in each of its gateways. If the call capacity usage in a particular gateway exceeds the high-water-mark threshold, the gatekeeper stops sending calls to that gateway. When the gateway's active call volume falls below the low-water-mark threshold, the gatekeeper resumes sending new calls to the gateway. These thresholds are global values and affect all gateways registered with a given gatekeeper.

If neither threshold is set, the gatekeeper uses the default values.

Examples

The following example sets the high and low call-volume thresholds for all of its gateways:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint resource-threshold onset 85 abatement 65
```

Related Commands

Command	Description
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

endpoint ttl

To enable the gatekeeper to assign a time-to-live (TTL) value to the endpoint when it registers with the gatekeeper, use the **endpoint ttl** *command in* gatekeeper configuration mode. To disable the TTL value, use the **no** form of this command.

endpoint ttl *time-to-live*

no endpoint ttl *time-to-live*

Syntax Description

time-to-live	TTL value, in seconds. Range is from 60 to 3600. The default is 1800.

Command Default

1800 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command specifies endpoint registration. Use this command to set the interval that the gatekeeper requires of an endpoint that does not supply its own value. Use a lower value to make the gatekeeper clear the registration of an unresponsive endpoint more quickly.

When an endpoint registers with the gatekeeper and does not provide a TTL value, the gatekeeper assigns this value as the time to live. When the TTL expires, the endpoint becomes subject to removal. However, the endpoint is queried a few times in an attempt to communicate with the device. If the device appears active, the registration does not expire. If the device is unresponsive after a few communication attempts, the endpoint is removed.

Examples

The following example enables a time to live value of 60 seconds:

```
endpoint ttl 60
```

Related Commands

Command	Description
timer cluster-element announce	Specifies the announcement period.
timer lrq seq delay	Specifies the timer for sequential LRQs.
timer lrq window	Specifies the window timer for LRQs.

erase vfc

To erase the Flash memory of a specified voice feature card (VFC), use the **erase vfc** command in privileged EXEC mode.

erase vfc *slot*

Syntax Description

slot	Slot on the Cisco AS5300 in which the specified VFC resides. Range is from 0 to 2. There is no default.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **erase vfc** command to erase the contents of Flash memory for a specified VFC (thereby freeing space in VFC Flash memory) including the default file list and the capability file list.

Examples

The following example erases the Flash memory on the VFC located in slot 0:

```
Router# erase vfc 0
```

Related Commands

Command	Description
delete vfc	Deletes a file from VFC Flash memory.

error-category

To specify Q.850 cause code mapping, use the **error-category** command in voice cause-code configuration mode. To disable Q.850 cause code mapping, use the **no** form of this command.

error-category *number* **q850-cause** *number*

no error-category *number* **q850-cause** *number*

Syntax Description

number	Specifies error category value to be mapped to a configured Q850 cause code value. Values range from 128 to 278.
q850-cause *number*	Specifies the default Q.850 cause code value. Values range from 1 to 127.

Command Default The IEC mechanism defaults to the assigned Q.850 cause codes.

Command Modes Voice cause-code configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Only the Session Initiation Protocol (SIP) and H.323 subsystems use the category and Q.850 mapping tables to determine the disconnect cause code when releasing a call due to an internal error.

To disable all mappings, use the no voice cause-code command. To disable a single mapping, use the voice cause-code command, followed by the no error-category *number* command.

Examples The following example sets error category 128 to map to Q.850 cause code 27:

```
Router(config)# voice cause code
Router(conf-voice-cause)# error-category 128 q850-cause 27
```

The following example defines two mappings for categories 128 and 129:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# error-category 128 q850-cause 27
Router(conf-voice-cause)# error-category 129 q850-cause 38
Router(conf-voice-cause)# exit
```

The following example removes the mapping for category 128 only, leaving 129 defined:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# no error-category 128
Router(conf-voice-cause)# exit
```

The following example removes all configured mappings:

```
Router(config)# no voice cause-code
```

Related Commands

Command	Description
show voice cause-code	Displays internal error category to q.850 cause code mapping.
voice cause-code	Enables voice cause-code configuration mode.

error-code-override

To configure the Session Initiation Protocol (SIP) error code to use at the dial peer for the call spike failure, use the **error-code-override** command in voice service SIP or dial peer voice configuration mode. To disable the SIP error code configuration, use the **no** form of this command.

error-code-override {**options-keepalive failure | call spike failure**} *sip-status-code-number*

no error-code-override {**options-keepalive failure | call spike failure**}

Syntax Description

options-keepalive failure	(Optional) Configures the SIP error code for options-keepalive failures.
call spike failure	(Optional) Configures the SIP error code for call spike failures.
sip-status-code-number	The SIP response error codec that is sent for the options-keepalive or call spike failure that happened at the dial peer. The range is from 400 to 699. The default value is 500. Table 1 in the "Usage Guidelines" section describes these error codes.

Command Default

The SIP error code is not configured.

Command Modes

Voice service SIP configuration (conf-ser-sip)
Dial peer voice configuration (conf-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The **call spike failure** keyword was introduced.

Usage Guidelines

The **error-code-override** command in voice service SIP or dial peer voice configuration mode configures the error code response for options-keepalive or call spike failures. The **voice-class sip error-code-override** command in voice service SIP or dial peer voice configuration mode configures the error code responses for call spike failures.

Table 1 describes the SIP error codes.

Table 23 SIP Error Codes

Error Code Number	Description
400	Bad Request
401	Unauthorized
402	Payment Required

Table 23 SIP Error Codes (continued)

Error Code Number	Description
403	Forbidden
404	Not Found
408	Request Timed Out
416	Unsupported URI
480	Temporarily Unavailable
482	Loop Detected
484	Address Incomplete
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
500–599	SIP 5xx—Server/Service Failure
500	Internal Server Error
502	Bad Gateway
503	Service Unavailable
600–699	SIP 6xx—Global Failure

Examples

The following example shows how to configure the SIP error code using the **error-code-override** command for options-keepalive failures in voice service SIP configuration mode:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(config-ser-sip)# error-code-override options-keepalive failure 503
```

The following example shows how to configure the SIP error code using the **error-code-override** command for call spike failures in dial peer voice configuration mode:

```
Router(config)# dial-peer voice 400
Router(conf-dial-peer)# error-code-override call spike failure 503
```

Related Commands

Command	Description
voice-class sip error-code-override	To configure the Session Initiation Protocol (SIP) error code that a dial peer uses for options-keepalive failures or call spike failures.

error-correction

To set error correction for the Signaling System 7 (SS7) signaling link when the SS7 Message Transfer Part Layer 2 (MTP2) variant is Bellcore or ITU-white, use the error-correction command in ITU configuration mode. To disable error correction, use the **no** form of this command.

error-correction [**basic** | **pcr** [**forced-retransmission** *parameters*]]

no error-correction

Syntax Description

basic	(Optional) Sets SS7 signaling link error correction to basic mode for configurations in which one-way propagation delay is less than 40 ms.
pcr	(Optional) Sets intercontinental SS7 signaling link error correction to Preventive Cyclic Retransmission (PCR) mode for configurations that are transmitted over satellite connections and for configurations in which one-way propagation delay is greater than 40 ms.
forced-retransmission	(Optional) Enables forced retransmission when the **pcr** keyword is selected. To disable forced retransmission, use the **no** form of the command.
parameters	(Optional) Sets the error-correction method for an SS7 signaling link. The following types of error correction are configurable: • **pcr-enabled**—Tracks the error-correction method on the SS7 signaling channel. The error-correction method can be either PCR or basic. PCR is disabled by default. • **forced-retransmission-enabled**—Tracks forced retransmission on the SS7 signaling channel. **Note** Forced retransmission is enabled only if PCR is enabled. • **n2** *octets*—The maximum number of N2 octets that can be queued in the RTB for an SS7 signaling channel before forced retransmission procedures are initiated. The number of octets can range from 200 to 4000. The default is 450. **Note** This parameter is ignored if forced retransmission is not enabled.

Command Default Error correction is set to basic.

Command Modes ITU configuration

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco 2600 series, Cisco AS5350, and Cisco AS5400 Cisco signaling link terminals (SLTs).

Usage Guidelines

The maximum supported signaling link loop (round trip) delay is 670 ms (the time between the sending of a message signal unit [MSU] and the reception of the acknowledgment for this MSU in undisturbed operation).

Examples

The following example sets the error-correction method to PCR and enables forced retransmission with the N2 parameter set and 1000 octets selected:

```
Router(config-ITU)# error-correction pcr forced-retransmission n2 1000
```

Related Commands

Command	Description
ss7 mtp2-variant	Configures an SS7 signaling link.

event-log

To enable event logging for applications, use the **event-log** command in application configuration monitor configuration mode. To disable event logging, use the **no** form of this command.

event-log [**size** [*number-of-events*]] [**one-shot**] [**pause**]

no event-log

Syntax Description

size [*number-of-events*]	(Optional) Maximum number of OSPF events in the event log.
one-shot	(Optional) Mode that enables the logging of new events at one specific point in time. The event logging mode is cyclical by default, meaning that all new events are logged as they occur.
pause	(Optional) Enables the user to pause the logging of any new events at any time, while keeping the current events in the log.

Command Default

By default, event logging is not enabled.
When event logging is enabled, it is cyclical by default.

Command Modes

Application configuration monitor configuration mode
OSPF for IPv6 router configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log** command.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command enables event logging globally for all voice applications. To enable or disable event logging for a specific application, use one of the following commands:

param event-log (application parameter configuration mode)

paramspace appcommon event-log (service configuration mode)

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20-percent, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30 percent. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event logging enabled:

```
application
 monitor
  event-log
```

The following example shows OSPF for IPv6 event logging enabled. The router instance is 1, the event-log size is 10,000, and the mode is one-shot.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
```

Related Commands

Command	Description
call application event-log	Enables event logging for all voice application instances.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log (Privileged EXEC)

To configure different event logging functions, use the **event-log** command in privileged EXEC mode.

event-log {**calibrate** | {**circular** | **platform-ticks**} {**off** | **on**} | {**disable** | **enable**} [*event-group*] | **init** | **mark** | **save** {*hostname* | *IP-address*} *prefix* | **timelog**}

Syntax Description

calibrate	Caliberates the platform clock.
circular	Enables or disables the circular event log.
off	Disables the circular event log.
on	Enables the circular event log.
disable	Disables event logging.
event-group	(Optional) Event group to be enabled or disabled. The range is from 1 to FFFFFFF.
enable	Enables event logging.
init	Initializes the event logging data structures.
mark	Marks an event log.
platform-ticks	Enables or disables platform ticks for a clock.
save	Saves the event log to the TFTP host as elog.out.
hostname	Hostname of the TFTP server to receive elog.out.
IP-address	IP address of the TFTP server to receive elog.out.
prefix	Prefix for the saved files.
timelog	Specifies time logging of 1000 events.

Command Default

Event logging functions are not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the circular event log:

```
Router# event-log circular on
```

Related Commands

Command	Description
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log dump ftp

To enable the gateway to write the contents of the application event log buffer to an external file, use the, use the **event-log dump ftp** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

event-log dump ftp *server[:port]/file username* **password** [*encryption-type*] *password*

no event-log dump ftp

Syntax Description

server	Name or IP address of FTP server where file is located.
port	(Optional) Specific port number on server.
file	Name and path of file.
username	Username required to access file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password	Password required to access file.

Command Default By default, this feature is not enabled on the gateway.

Command Modes Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log dump ftp** command.

Usage Guidelines This command enables the gateway to automatically write the event log buffer to the named file either after an active application instance terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **event-log max-buffer-size** command in application configuration monitor mode.

Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Examples

The following example enables the gateway to write application event logs to an external file named app_elogs.log on a server named ftp-server:

```
application
monitor
 event-log dump ftp ftp-server/elogs/app-elogs.log username myname password 0 mypass
```

The following example specifies that application event logs are written to an external file named app_elogs.log on a server with the IP address of 10.10.10.101:

```
application
monitor
 event-log dump ftp 10.10.10.101/elogs/app-elogs.log username myname password 0 mypass
```

Related Commands

Command	Description
call application event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log	Enables event logging for applications.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.

event-log error-only

To restrict event logging to error events only for application instances, use the **event-log error-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

event-log error-only

no event-log error-only

Syntax Description This command has no arguments or keywords.

Command Default If logging is enabled, all application events are logged.

Command Modes Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log error-only** command.

Usage Guidelines

- This command limits new event logging to error events only; it does not enable logging.

You must use this command with either the **event-log** command, which enables event logging for all voice applications, or enable event logging for a specific application using the **param event-log** command (package appcommon configuration mode) or the **paramspace appcommon event-log** command (service configuration mode).

- Any events logged before this command is issued are not affected.

Examples The following example enables event logging for error events only:

```
application
monitor
 event-log
 event-log error-only
```

Related Commands

Command	Description
call application event-log error-only	Restricts event logging to error events only for application instances.
event-log	Enables event logging for applications.

Command	Description
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance

event-log max-buffer-size

To set the maximum size of the event log buffer for each application instance, use the **event-log max-buffer-size** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

event-log max-buffer-size *kbytes*

no event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range is 1 to 50. Default is 4 KB.

Command Default

By default, the maximum size is set to 4 KB.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log max-buffer-size** command.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application session-level** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Note

- Do not set the maximum buffer size to more than you need for a typical application session. After an active session terminates, the amount of memory used by the buffer is allocated to the history table and is maintained for the length of time set by the **history session retain-timer** command. Also consider that most fatal errors are captured at the end of an event log.
- To conserve memory resources, write the event log buffer to FTP by using the **event-log dump ftp** command.

Examples

The following example sets the application event log buffer to 8 KB:

```
application
 monitor
 event-log max-buffer-size 8
```

Related Commands

Command	Description
event-log	Enables event logging for applications.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
call application event-log max-buffer-size	Maximums size of the event log buffer for each application instance.

expect-factor

To set the expect-factor value for voice quality, which affects the threshold calculated planning impairment factor (ICPIF) loss/delay busyout value, use the **expect-factor** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

expect-factor *value*

no expect-factor *value*

Syntax Description

value	Integers that represent quality of voice as described in ITU G.107. Range: 0 to 20, with 0 representing toll quality. Default: 10.

Command Default 10

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(8)T	The *value* default changed from 10 to 0.
12.3(3)T	The *value* default changed from 0 to 10.

Usage Guidelines The expect factor impacts the calculated value of ICPIF. This value is used in conjunction with Simple Network Management Protocol (SNMP) to generate a trap when voice quality falls below a configured value. It also impacts the value of ICPIF reported in call-account records as well as in call-history values on the gateway.

Use this and related commands together on a dial peer as follows:

- Use this command to set the expect-factor value.
- Use the **icpif** command to set a threshold ICPIF value (the ICPIF calculation uses the expect-factor value as well as values for loss and delay).
- Use the **snmp enable peer-trap poor-qov** command to generate notifications in the form of SNMP traps to the network manager for calls whose ICPIF value exceeds the threshold.

Note For more information on ICPIF, see *IP SLAs—Analyzing VoIP Service Levels Using the VoIP Jitter Operation* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsla_c/hsvoipj.htm

Examples The following example sets the expect factor for a dial peer:

```
dial-peer voice 10 voip
 expect-factor 0
```

Related Commands

Command	Description
icpif	Specifies the ICPIF threshold for calls sent by a dial peer.
snmp enable peer-trap poor-qov	Generates poor-quality-of-voice notifications for applicable calls associated with a VoIP dial peer.

extsig mgcp

To configure external signaling control by Media Gateway Control Protocol (MGCP) for a T1 or E1 trunk controller card, use the **extsig mgcp** command in controller configuration mode. To discontinue MGCP control for this controller, use the **no** form of this command.

extsig mgcp

no extsig mgcp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Controller configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

For T3 lines, each logical T1 trunk controller card must be configured using the **extsig mgcp** command.

Examples

The following example shows MGCP signaling control being configured for T1 controller 7/0:

```
controller T1 7/0
 framing esf
 extsig mgcp
 guard-timer 10 on-expiry reject
 linecode b8zs
 ds0-group 1 timeslots 1-24 type none service mgcp
```

Related Commands

Command	Description
dialer extsig	Configures an interface to initiate and terminate calls using an external signaling protocol.

Cisco IOS Voice Commands: F

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

fax interface-type

To specify the interface to be used for a fax call, use the **fax interface-type** command in global configuration mode. To reset to the default fax protocol, use the **no** form of this command.

fax interface-type {**fax-mail** | **modem** | **vfc**}

no fax interface-type {**fax-mail** | **modem** | **vfc**}

Syntax Description

fax-mail	Specifies that voice digital signal processors (DSPs) process fax store-and-forward data. This keyword replaces the **vfc** keyword for DSPs.
modem	(Cisco AS5300 only) Specifies that modem cards process fax store-and-forward data. **Note** This keyword is not supported except for instances documented in the "Usage Guidelines" section.
vfc	(Cisco AS5300 only) Specifies that voice feature cards (VFCs) process fax store-and-forward data. This keyword has been superseded by the **fax-mail** keyword and is retained for backward compatibility only.

Command Default

Cisco AS5300: See the "Usage Guidelines" section
All other platforms: **fax-mail**

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	The command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on Cisco 1750 and the **fax-mail** keyword was added.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

When using this command to change the interface type for store-and-forward fax, you must reload (reboot or reset) the router.

On the Cisco AS5300 access server, the keyword **vfc** maps internally to the **fax-mail** keyword. If you use the **vfc** keyword with the **fax interface-type** command, the output from the **show running-config** command displays **fax-mail** as the option that was set.

The Cisco AS5300 defaults for the **fax interface-type** command are as follows:

- If the Cisco AS5300 has voice cards only, the default is the **fax-mail** keyword. The **modem** keyword is unavailable.
- If the Cisco AS5300 has modem cards only, the default is the **modem** keyword.
- If the Cisco AS5300 has both modem and voice cards, the default is the **modem** keyword.

Examples

The following example specifies the use of voice DSPs to process fax store-and-forward data:

```
Router(config)# fax interface-type fax-mail
```

The following example specifies the use of modems to process fax store-and-forward data on a Cisco AS5300:

```
Router(config)# fax interface-type modem
```

fax protocol (dial peer)

To specify the fax protocol to be used for a specific VoIP dial peer, use the **fax protocol** command in dial peer configuration mode. To return to the global default fax protocol, use the **system** keyword or the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850

fax protocol {**none** | **system** | **pass-through** {**g711ulaw** | **g711alaw**}}

no fax protocol

All Other Platforms

fax protocol {**cisco** | **none** | **system** | **pass-through** {**g711ulaw** | **g711alaw**}}

no fax protocol

Syntax Description

cisco	Cisco-proprietary fax protocol.
none	No fax pass-through is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through** command.
system	Uses the global configuration that was set using the **fax protocol** command in voice-service configuration mode.
pass-through	The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**—Uses the G.711 u-law codec. • **g711alaw**—Uses the G.711 a-law codec.

Command Default

system

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800. The **none** keyword was introduced.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.

Release	Modification
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The **t.38** keyword and its options were moved to two new commands: **fax protocol t38** (dial peer) and **fax protocol t38** (voice-service).

Usage Guidelines

Use the **fax protocol** command in dial-peer configuration mode to configure the type of fax relay capability for a specific dial peer. Note the following command behavior:

- **fax protocol none**—Disables all fax handling.
- **no fax protocol**—Sets the fax protocol for the dial peer to the default, which is **system**.

If the **fax protocol** (voice-service) command is used to set fax relay options for all dial peers and the **fax protocol** (dial peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

Examples

The following example specifies that the fax stream use fax pass-through for VoIP dial peer 99:

```
dial-peer voice 99 voip
 fax protocol pass-through g711ulaw
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.

fax protocol (voice-service)

To specify the global default fax protocol to be used for all VoIP dial peers, use the **fax protocol** command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850

fax protocol {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}

no fax protocol

All Other Platforms

fax protocol {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}

no fax protocol

Syntax Description

none	No fax pass-through is attempted. All special fax handling is disabled, except for modem pass-through (if configured with the **modem pass-through** command).
pass-through	The fax stream uses one of the following high-bandwidth codecs: • **g711alaw**—Uses the G.711 A-law codec. • **g711ulaw**—Uses the G.711 mu-law codec.
cisco	Cisco-proprietary fax protocol. The **cisco** keyword is the default for all platforms except the Cisco AS5350, Cisco AS5400, and Cisco AS5850. • This is the only valid option when you are using Cisco Unified CME 4.0(3) or a later version on Skinny Call Control Protocol (SCCP)-controlled FXS ports.

Command Default

If no fax protocol is specified, the **cisco** protocol is the default for all platforms except the Cisco AS5350, Cisco AS5400, and Cisco AS5850. For these three platforms, **none** is the default, so no fax pass-through is attempted.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The **t.38** keyword and its options were removed and added to two new commands: **fax protocol t38 (dial peer)** and **fax protocol t38 (voice-service)**.
12.4(11)T	Support for SCCP-controlled FXS ports was added.

Usage Guidelines

Use the **fax protocol** command with the **voice service voip** command to configure the fax relay capability for all VoIP dial peers.

Note the following command behavior:

- **fax protocol none**— Disables all fax handling.
- **no fax protocol**—Sets the fax protocol to the default.

If the **fax protocol** (voice-service) command is used to set fax relay options for all dial peers and the **fax protocol** (dial peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer. When the **system** keyword is used in the dial-peer configuration of the **fax protocol** command, it specifies that the global default fax protocol set with this command is used by that dial peer.

In Cisco Unified CME 4.0(3) and later, the **fax protocol cisco** (voice-service) command is the only supported fax protocol option for SCCP-controlled FXS ports. G.711 fax pass-through is not supported for Cisco VG 224 and FXS ports.

Note The **modem passthrough protocol** and **fax protocol** commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message.

The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol passthrough** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.

Note Even though the **modem passthrough protocol** and **fax protocol passthrough** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol** command to the **modem passthrough nse** command, the configured **fax protocol passthrough** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Examples

The following example specifies that the fax stream for all VoIP dial peers use fax pass-through:

```
voice service voip
 fax protocol pass-through g711ulaw
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
modem passthrough	Enables fax or modem pass-through over VoIP globally for all dial peers.
voice service voip	Enters voice-service configuration mode.

fax protocol t38 (dial peer)

To specify the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer, use the **fax protocol t38** command in dial-peer configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850 Platforms

fax protocol t38 [**nse** [**force**]] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

no fax protocol t38

All Other Platforms

fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

no fax protocol t38

Syntax Description

nse	(Optional) Uses NSEs to switch to T.38 fax relay.
force	(Optional) Unconditionally, uses Cisco network services engines (NSE) to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
version {**0** | **3**}	(Optional) Specifies a version for configuring fax speed: • **0**—Configures version 0, which uses T.38 version 0 (1998—G3 faxing) • **3**—Configures version 3, which uses T.38 version 3 (2004—V.34 or SG3 faxing)
ls-redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. For details, see to command-line interface (CLI) help. Default is 0.
hs-redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. For details, see the command-line interface (CLI) help. Default is 0.
fallback	(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
cisco	(Optional) Cisco-proprietary fax protocol.
none	(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through** command.
pass-through	(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**—Uses the G.711 mu-law codec. • **g711alaw**—Uses the G.711 a-law codec.

Command Default **ls-redundancy 0 hs-redundancy 0 fallback none** for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms
ls-redundancy 0 hs-redundancy 0 fallback cisco for all other platforms

Command Modes Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.1(1)T	This command was modified. The **version** keyword was added with the **0** and **3** keywords to specify fax speed as G3 or SG3.

Usage Guidelines Use this command in dial-peer configuration mode to configure the type of fax relay capability for a specific dial peer. If the **fax protocol t38 (voice-service)** command is used to set fax relay options for all dial peers and the **fax protocol t38 (dial peer)** command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

If you specify **version 3** in the **fax protocol t38** command and negotiate T.38 version 3, the fax rate is automatically set to 33600.

The **ls-redundancy** and **hs-redundancy** keywords are used to send redundant T.38 fax packets. Setting the **hs-redundancy** keyword to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Use the **nse force** option when the H.323 or SIP gateway is interoperating with a Cisco MGCP gateway and the call agent does not support the interworking and negotiation of T.38 fax relay and NSE attributes at the time of call setup. When the corresponding option is configured on the MGCP gateway, the **nse force** option allows T.38 fax relay to be used between Cisco H.323 or SIP gateways and MGCP gateways.

Examples The following example show how to configure T.38 fax relay for VoIP:

```
dial-peer voice 99 voip
 fax protocol t38
```

The following example shows how to use NSEs to enter T.38 fax relay mode:

```
dial-peer voice 99 voip
 fax protocol t38 nse
```

The following example shows how to specify the T.38 fax protocol for this dial peer, set low-speed redundancy to a value of 1, and set high-speed redundancy to a value of 0:

```
dial-peer voice 99 voip
 fax protocol t38 ls-redundancy 1 hs-redundancy 0
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.

fax protocol t38 (voice-service)

To specify the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers, use the **fax protocol t38** command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850 Platforms

fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

no fax protocol t38

All Other Platforms

fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

no fax protocol t38

Syntax Description

nse	(Optional) Uses network services engines (NSE) to switch to T.38 fax relay.
force	(Optional) Unconditionally, uses Cisco NSEs to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
version {**0** | **3**}	(Optional) Specifies a version for configuring fax speed: • **0**—Configures version 0, which uses T.38 version 0 (1998—G3 faxing) • **3**—Configures version 3, which uses T.38 version 3 (2004—V.34 or SG3 faxing)
ls-redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. For details, refer to command-line interface (CLI) help. Default is 0.
hs-redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. For details, refer to the command-line interface (CLI) help. Default is 0.
fallback	(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
cisco	(Optional) Cisco-proprietary fax protocol.
none	(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through** command.
pass-through	(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**—Uses the G.711 mu-law codec. • **g711alaw**—Uses the G.711 a-law codec.

Command Default

ls-redundancy 0 hs-redundancy 0 fallback none for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms
ls-redundancy 0 hs-redundancy 0 fallback cisco for all other platforms

Command Modes

Voice-service configuration (config-voi-srv)

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.1(1)T	This command was Modified. The **version** keyword was added with the **0** and **3** keywords to specify fax speed.

Usage Guidelines

Use the **fax protocol t38** command and the **voice service voip** command to configure T.38 fax relay capability for all VoIP dial peers. If the **fax protocol t38** (voice-service) command is used to set fax relay options for all dial peers and the **fax protocol t38** (dial-peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

If you specify **version 3** in the **fax protocol t38** command and negotiate T.38 version 3, the fax rate is automatically set to 33600.

The **ls-redundancy** and **hs-redundancy** keywords are used to send redundant T.38 fax packets. Setting the **hs-redundancy** keyword to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Use the **nse force** option when the H.323 or SIP gateway is interoperating with a Cisco MGCP gateway and the call agent does not support the interworking and negotiation of T.38 fax relay and NSE attributes at the time of call setup. When the corresponding option is configured on the MGCP gateway, the **nse force** option allows T.38 fax relay to be used between Cisco H.323 or SIP gateways and MGCP gateways.

Note Do not use the **cisco** keyword for the fallback option if you specified **version 3** for SG3 fax transmission.

Examples

The following example shows how to configure the T.38 fax protocol for VoIP:

```
voice service voip
 fax protocol t38
```

The following example shows how to use NSEs to unconditionally enter T.38 fax relay mode:

```
voice service voip
 fax protocol t38 nse
```

The following example shows how to specify the T.38 fax protocol for all VoIP dial peers, set low-speed redundancy to a value of 1, and set high-speed redundancy to a value of 0:

```
voice service voip
 fax protocol t38 ls-redundancy 1 hs-redundancy 0
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
voice service voip	Enters voice-service configuration mode.

fax rate (dial peer)

To establish the rate at which a fax is sent to a specified dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer for voice calls, use the **no** form of this command.

fax rate {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**} {**disable** | **voice**} [**bytes** *milliseconds*]

no fax rate

Syntax Description

2400	2400 bits per second (bps) fax transmission speed.
4800	4800 bps fax transmission speed.
7200	7200 bps fax transmission speed.
9600	9600 bps fax transmission speed.
12000	12000 bps fax transmission speed.
14400	14400 bps fax transmission speed.
disable	Disables fax relay transmission capability.
voice	Highest possible transmission speed allowed by the voice rate.
bytes *milliseconds*	(Optional) Specifies fax packetization rate, in milliseconds. Range is 20 to 48. Default is 20. • For Cisco fax relay, this keyword-argument pair is valid only on Cisco 2600 series, Cisco 3600 series, Cisco AS5300, and Cisco 7200 series routers. • For T.38 fax relay, this keyword-argument pair is valid only on Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers. For other routers, the packetization rate for T.38 fax relay is fixed at 40 ms and cannot be changed.

Command Default Voice rate

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced as the **fax-rate** command on the Cisco 3600.
12.0(2)XH	The **12000** keyword was added.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T and implemented on the Cisco MC3810.
12.1(3)T	The command name changed from **fax-rate** to **fax rate** (nonhyphenated).
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Use this command to specify the fax transmission rate to the specified dial peer.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but monopolize a significantly large portion of the available bandwidth. The lower transmission speed values (2400 bps) provide a slower transmission speed and use a relatively smaller portion of the available bandwidth.

Note The fax call is not compressed using the **ip rtp header-compression** command because User Datagram Protocol (UDP) is being used and not Real-Time Transport Protocol (RTP). For example, a 9600 bps fax call takes approximately 24 kbps.

If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission is above the bandwidth reserved for Resource Reservation Protocol (RSVP).

Tip Because a large portion of the available network bandwidth is monopolized by the fax transmission, Cisco does not recommend setting the fax rate value higher than the value of the selected codec. If the fax rate value is set lower than the codec value, faxes take longer to send but use less bandwidth.

The **voice** keyword specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, the fax transmission may occur at a rate up to 14,400 bps because 14,400 bps is less than the 64k voice rate. If the voice codec is G.729 (8k), the fax transmission speed is 7200 bps.

Examples

The following example configures a fax rate transmission speed of 9600 bps for faxes sent using a dial peer:

```
dial-peer voice 100 voip
 fax rate 9600 voice
```

The following example sets a fax rate transmission speed at 12,000 bps and the packetization rate at 20 milliseconds:

fax rate 12000 bytes 20

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.

fax rate (pots)

To establish the rate at which a fax is sent to the specified plain old telephone service (POTS) dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer to handle only voice calls, use the **no** form of this command.

fax rate {**disable** | **system** | **voice**}

no fax rate

Syntax Description

disable	Disables fax-relay transmission capability.
system	Uses rate choice specified in global fax rate CLI under the **voice service pots** command.
voice	Highest possible transmission speed allowed by the voice rate for this dial peer. For example, if the voice codec is G.711, fax transmission may occur at a rate of up to 14,400 bps.

Command Default System

Command Modes dial peer configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on the following platforms: Cisco 1700 series, Cisco 3600 series, and Cisco ICS 7750.

Usage Guidelines This implementation of the **fax rate** command is only applicable to POTS dial peers.

Examples The following example shows a fax rate transmission set to **voice** on POTS dial peer 1:

```
dial-peer voice 1 pots
 fax rate voice
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
fax rate (voip)	Establishes the rate at which a fax is sent to the specified VoIP dial peer.

fax rate (voice-service)

To establish the rate at which a fax is sent for POTS-to-POTS voice calls, use the **fax rate** command in voice-service configuration mode. To reset for voice only calls, use the **no** form of this command.

fax rate {**disable** | **voice**}

no fax rate

Syntax Description

disable	Disables fax relay transmission capability.
voice	Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission may occur at a rate of up to 14400 bps.

Command Default **fax rate voice** command behavior is enabled by default

Command Modes Voice-service configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on the following platforms: Cisco 1700 series, Cisco 3600 series, and Cisco ICS 7750.
12.3(4)T	This command was modified so that the "fax rate voice" setting is the default setting for the **fax rate** command in voice-service configuration mode and, hence, will no longer be displayed in the running configuration.

Usage Guidelines This implementation of the **fax rate** command applies only when voice service is set to POTS. Although **fax rate voice** command behavior is the default setting, you must specify this functionality in voice-service configuration mode in order to establish the rate at which a fax is sent for POTS-to-POTS voice calls. If you do not configure **fax rate voice** functionality and you do not specify **fax rate disable** command behavior, fax calls are processed as a regular voice calls and their completion is subject to line quality just like any other form of voice communication.

Note Because the **fax rate voice** command has been reclassified as a default setting, it will no longer automatically generate an entry in your gateway router's running configuration in NVRAM. If your gateway configuration requires **fax rate voice** command functionality, you must reconfigure your gateway after loading a Cisco IOS image earlier than Cisco IOS Release 12.3(4)T.

Examples The following example shows voice service fax rate transmission set to **disable**:

```
voice service pots
 fax rate disable
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol for all VoIP dial peers.
voice service	Specifies the voice encapsulation type.

fax receive called-subscriber

To define the called subscriber identification (CSI), use the **fax receive called-subscriber** command in global configuration mode. To disable the configured CSI, use the **no** form of this command.

fax receive called-subscriber {**d** | *telephone-number*}

no fax receive called-subscriber {**d** | *telephone-number*}

Syntax Description

d	Wildcard that indicates that the information displayed is captured from the configured destination pattern.
telephone-number	Destination telephone number. Valid entries are the plus sign (+), numerals from 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, you must use the plus sign as the first character.

Command Default

Enabled with a null string

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to define the number displayed in the liquid crystal display (LCD) of the sending fax device when you are sending a fax to a recipient. Typically, with a standard Group 3 fax device, this is the telephone number associated with the receiving fax device. The command defines the CSI.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures the number 555-0134 as the called subscriber number:

```
fax receive called-subscriber 5550134
```

fax-relay (dial peer)

To allow for the suppression of tones from the fax machine side so that Super Group 3 (SG3) fax machines can negotiate down to G3 speeds using fax relay or to disable fax-relay Error Correction Mode (ECM) on a VoIP dial peer, use the **fax-relay** command in dial peer configuration mode. To disable these functions, use the **no** form of this command.

fax-relay {**ans-disable** | **ecm-disable** | **sg3-to-g3** [*system*]}

no fax-relay {**ans-disable** | **ecm-disable** | **sg3-to-g3** [*system*]}

Syntax Description

ans-disable	Suppresses ANS tones from originating SG3 fax machines so that these machines can operate at G3 speeds using fax relay.
ecm-disable	Disables fax-relay ECM on a VoIP dial peer.
sg3-to-g3	Allows SG3 machines to negotiate down to G3 speeds using fax relay.
system	(Optional) The protocol set to be used in the voice-service configuration mode.

Command Default

If this command is not enabled, modem upspeed can occur when ANS tones are detected, fax-relay ECM is enabled, and SG3-to-SG3 fax relay communication is not supported and probably will fail.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(3)T	This command was introduced as the **fax-relay ecm-disable** command.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(4)T	The **sg3-to-g3** keyword and *system* argument were added.
12.4(6)T	This command was implemented on the Cisco 1700 series and Cisco 2800 series.
12.4(20)T1	The **ans-disable** keyword was added.

Usage Guidelines

The **ans-disable** keyword was added to ensure that modem upspeed does not occur when an ANS tone is detected. When the **fax-relay ans-disable** command is entered, the modem-related sessions fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **fax-relay ecm-disable** command is entered, the DSP fax-relay firmware disables ECM by modifying the Digital Information Signal (DIS) T.30 message. This is performed on DIS signals in both directions so that ECM is disabled in both directions even if only one gateway is configured with ECM disabled. This setting is provisioned when the DSP channel starts fax relay and cannot be changed during the fax relay session.

When the **fax-relay sg3-to-g3** command is entered, the DSP fax-relay firmware suppresses the V.8 call menu (CM) tone and the fax machines negotiate down to G3 speeds for the fax stream. Modem communication is impacted if the session does not negotiate either modem passthrough or relay. Use this command for H.323 and Session Initiation Protocol (SIP) signaling types.

The **fax-relay** command is also available in voice-service configuration mode, but the **ecm-disable** keyword and *system* argument are not available.

Examples

The following dial-peer configuration disables ECM on the voice dial peer:

```
Router(config)# dial-peer voice 25 voip
Router(config-dial-peer)# fax-relay ecm-disable
```

The following dial-peer configuration shows SG3 V.8 fax CM message suppression being enabled on the voice dial peer for H.323 and SIP signaling types:

```
Router(config)# dial-peer voice 25 voip
Router(config-dial-peer)# fax-relay sg3-to-g3
```

The following dial-peer configuration shows how to enable ANS tone squelching at the DSP level for all VoIP dial peers:

```
Router(config)# dial-peer voice 25 voip
Router(config-dial-peer)# fax-relay ans-disable
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol to be used for a specific VoIP dial peer.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
fax-relay (voice-service)	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay and to enable the fax stream between two SG3 fax machines to negotiate down to G3 speeds on a VoIP dial peer.
mgcp fax-relay	Allow ANS tones to be disabled for SG3 machines to operate at G3 speeds for MGCP fax relay or to enable the fax stream between two SG3 fax machines to negotiate down to G3 speeds for MGCP fax relay.

fax send center-header

To specify the data that appears in the center position of the fax header information, use the **fax send center-header** command in global configuration mode. To remove the selected options, use the **no** form of this command.

fax send center-header {**a** | **d** | **p** | **s** | **t** | *string*}

no fax send center-header {**a** | **d** | **p** | **s** | **t** | *string*}

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender's address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides personalized information. Valid characters are any text plus wildcards—for example, Time:t. There is no default.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Mail messages that contain only text or contain text attachments (text of the MIME media type) can be converted by the off-ramp gateway into a format understood by a fax machine's text-to-fax converter. When this conversion is performed, this command indicates what header information is added to the center top position of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers.

Note Faxed header information cannot be converted from TIFF files to standard fax transmissions.

This command lets you configure several options by combining one or more wildcards with text string information to customize your fax header information.

Note If the information you have selected for the **fax send center-header** command exceeds the space allocated for the center fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example selects the fax transmission time as the centered fax header:

```
fax send center-header $t$
```

The following example configures the company name “Widget” and its address as the centered fax header:

```
fax send center-header widget $s$
```

Related Commands

Command	Description
fax send left-header	Specifies the data that appears on the left in the fax header.
fax send right-header	Specifies the data that appears on the right in the fax header.

fax send coverpage comment

To define customized text for the title field of a fax cover sheet, use the **fax send coverpage comment** command in global configuration mode. To disable the defined comment, use the **no** form of this command.

fax send coverpage comment *string*

no fax send coverpage comment *string*

Syntax Description

string	Text string that adds customized text in the title field of the fax cover sheet. Valid characters are any ASCII characters.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command can be overridden by the **fax send coverpage e-mail-controllable** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example configures an individualized title comment of "XYZ Fax Services" for generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage comment XYZ Fax Services
```

Related Commands

Command	Description
fax send coverpage e-mail-controllable	Controls the cover page generation on a per-recipient basis, based on the information contained in the destination address of the e-mail message.
fax send coverpage enable	Generates fax cover sheets.
fax send coverpage show-detail	Prints all of the e-mail header information as part of the fax cover sheet.

fax send coverpage e-mail-controllable

To defer to the cover page setting in the e-mail header to generate a standard fax cover sheet, use the **fax send coverpage e-mail-controllable** command in global configuration mode. To disable standard fax sheet generation, use the **no** form of this command.

fax send coverpage e-mail-controllable

no fax send coverpage e-mail-controllable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

You can also use the destination address of an e-mail message to control the cover page generation on a per-recipient basis. Use this command to configure the router to defer to the cover page setting in the e-mail header.

In essence, the off-ramp router defers to the setting configured in the e-mail address itself. For example, if the address has a parameter set to cover=no, this parameter overrides the setting for the **fax send coverpage enable** command, and the off-ramp gateway does not generate and send a fax cover page. If the address has a parameter set to cover=yes, the off-ramp gateway defers to this parameter setting to generate and send a fax cover page.

Table 24 shows examples of what the user would enter in the To: field of the e-mail message.

Table 24 Sample Entries for the To: Field

To: Field Entries	Description
`FAX=+1-312-555-3260@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. If the **fax coverpage enable** command is entered, store-and-forward fax generate a fax cover page.

Table 24 Sample Entries for the To: Field (continued)

To: Field Entries	Description
`FAX=+1-312-555-3260/cover=no@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=no statement. No cover page is generated.
`FAX=+1-312-555-3260/cover=yes@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=yes statement. Store-and-forward fax generates a fax cover page.

Note This command applies to off-ramp store-and-forward fax functions.

Examples

The following example enables standard generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage e-mail-controllable
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.
fax send coverpage enable	Generates fax cover sheets.
fax send coverpage show-detail	Prints all the e-mail header information as part of the fax cover sheet.

fax send coverpage enable

To generate fax cover sheets for faxes that were converted into e-mail messages, use the **fax send coverpage enable** command in global configuration mode. To disable fax cover sheet generation, use the **no** form of this command.

fax send coverpage enable

no fax send coverpage enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines This command applies to off-ramp store-and-forward fax functions.

Note This command is applicable only to faxes that were converted to e-mail messages. The Cisco AS5300 universal access server does not alter fax TIFF attachments. Therefore you cannot use this command to enable the Cisco AS5300 to generate fax cover pages for faxes that are converted from TIFF files to standard fax transmissions.

Examples The following example enables the generation of fax cover sheets:

```
fax send coverpage enable
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.
fax send coverpage e-mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet
fax send coverpage show-detail	Prints all the e-mail header information as part of the fax cover sheet.

fax send coverpage show-detail

To display all e-mail header information as part of the fax cover sheet, use the **fax send coverpage show-detail** command in global configuration mode. To prevent the e-mail header information from being displayed, use the **no** form of this command.

fax send coverpage show-detail

no fax send coverpage show-detail

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guideliness This command applies to off-ramp store-and-forward fax functions.

Note This command is applicable only to faxes that are converted to e-mail messages. The Cisco AS5300 universal access server does not alter fax TIFF attachments. Therefore, you cannot use this command to enable the Cisco AS5300 to display additional fax cover page information for faxes that are converted from TIFF files to standard fax transmissions.

Examples The following example configures an individualized generated fax cover sheet that contains the e-mail header text:

```
fax send coverpage enable
no fax send coverpage e-mail-controllable
fax send coverpage show-detail
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.
fax send coverpage e-mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet.
fax send coverpage enable	Generates fax cover sheets.

fax send left-header

To specify the data that appears on the left in the fax header, use the **fax send left-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

fax send left-header {**a** | **d** | **p** | **s** | **t** | *string*}

no fax send left-header {**a** | **d** | **p** | **s** | **t** | *string*}

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender's address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides customized information. Valid characters are any combination of ASCII characters and the wildcards listed above.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Mail messages that contain only text or text attachments (text of MIME media type) can be converted by the off-ramp device into a format understood by fax machines using a text-to-fax converter. When this conversion is performed, the **fax send left-header** command is used to indicate what header information should be added to the top left of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers, and the Cisco IOS software does not modify TIFF attachments.

This command lets you configure several options at once by combining one or more wildcards with text string information to customize your fax header information.

If the information you select for the **fax send left-header** command exceeds the space allocated for the left fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example puts the fax transmission time on the left side of the fax header:

```
fax send left-header $t$
```

The following example puts the company name “widget” and its address on the left side of the fax header:

```
fax send left-header widget $s$
```

Related Commands

Command	Description
fax send center-header	Specifies the data that appears in the center of the fax header.
fax send right-header	Specifies the data that appears on the right in the fax header.

fax send max-speed

To specify the maximum speed at which an outbound fax is transmitted, use the **fax send max-speed** command in global configuration mode. To disable the selected speed, use the **no** form of this command.

fax send max-speed {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**}

no fax send max-speed {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**}

Syntax Description

2400	Transmission speed of 2400 bits per second (bps).
4800	Transmission speed of 4800 bps.
7200	Transmission speed of 7200 bps.
9600	Transmission speed of 9600 bps.
12000	Transmission speed of 12,000 bps.
14400	Transmission speed of 14,400 bps. This is the default.

Command Default

14,400 bps

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example sets the outbound fax transmission rate at 2400 bps:

```
fax send max-speed 2400
```

fax send right-header

To specify the data that appears on the right in the fax header information, use the **fax send right-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

fax send right-header {**a** | **d** | **p** | **s** | **t** | *string*}

no fax send right-header {**a** | **d** | **p** | **s** | **t** | *string*}

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides customized information. Valid characters are any combination of ASCII characters and the wildcards listed above.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Mail messages that contain only text or text attachments (text of MIME media type) can be converted by the off-ramp device into a format understood by fax machines using the text-to-fax converter. When this conversion is performed, this command is used to indicate what header information should be added to top right of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers, and the Cisco IOS software does not modify TIFF attachments.

This command lets you configure several options at once by combining one or more wildcards with text string information to customize your fax header information.

Note If the information you select for the **fax send right-header** command exceeds the space allocated for the right fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example puts the fax date in the right-hand side of the fax header:

```
fax send right-header $a$
```

The following example puts the company name "XYZ" and its address in the right-hand side of the fax header:

```
fax send right-header XYZ $s$
```

Related Commands

Command	Description
fax send center-header	Specifies the data that appears in the center in the fax header.
fax send left-header	Specifies the data that appears on the left in the fax header.

fax send transmitting-subscriber

To define the transmitting subscriber information (TSI), use the **fax send transmitting-subscriber** command in global configuration mode. To disable the configured value, use the **no** form of this command.

fax send transmitting-subscriber {**s** | *string*}

no fax send transmitting-subscriber {**s** | *string*}

Syntax Description

s	Wildcard that inserts the sender name from the RFC 822 header (captured by the on-ramp device from the sending fax machine) in the selected position.
string	Originating telephone number. Valid entries are the plus sign (+), numerals from 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, you must use the plus sign as the first character.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines The transmitting subscriber number is the number of the originating fax and is displayed in the LCD of the receiving fax device. Typically, with a standard Group 3 fax device, this number is the telephone number associated with the transmitting or sending fax device. This command defines the TSI.

This command applies to off-ramp store-and-forward fax functions.

Examples The following example configures the company number as captured by the on-ramp device from the sending fax machine:

```
fax send transmitting-subscriber +14085550134
```

file-acct flush

To manually flush call detail records (CDRs) from the buffer to the accounting file, use the **file-acct flush** command in privileged EXEC mode.

file-acct flush {**with-close** | **without-close**}

Syntax Description

with-close	Call records are appended to the accounting file and the file is closed.
without-close	Call records are appended to the accounting file and the file remains open.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command if you need to manually flush the buffer, for example, if flash becomes full or you do not want to wait until the buffer is automatically flushed. This command immediately flushes the buffer and appends all CDRs in the buffer to the current accounting file. CDRs are automatically flushed from the buffer and written to the file whenever there is enough data based on the **maximum buffer-size** command or after the timer set with the **maximum cdrflush-timer** command expires.

Using the **with-close** keyword closes the current file and opens a new file after appending the records. Using the **without-close** keyword leaves the current file open after appending the records.

Examples

The following example appends the records to the accounting file and closes the file:

```
file-acct flush with-close
```

Related Commands

Command	Description
gw-accounting	Enables an accounting method for collecting CDRs.
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

file-acct reset

To manually switch back to the primary device for file accounting, use the **file-acct reset** command in privileged EXEC mode.

file-acct reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command allows you to switch back to the primary device when it becomes available if the backup device is currently being used because the primary device failed.

If the file transfer to the primary device fails, the file accounting process retries the primary device up to the number of times defined by the **maximum retry-count** command and then switches to the secondary device defined with the **secondary** command. This command flushes the buffer and writes the call detail records (CDRs) to the currently active file before resetting to the primary device and opening a new file.

If the secondary device also fails, the accounting process ends and the system logs an error. New CDRs are dropped until one device comes back online and you use this command. The system then immediately resets to the primary device, if available.

Examples

The following example shows how to switch back to the primary device:

```
Router# file-acct reset
```

Related Commands

Command	Description
gw-accounting	Enables an accounting method for collecting CDRs.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

filter voice

To specify that voice calls bypass authentication, authorization, and accounting (AAA) preauthentication, use the **filter voice** command in AAA preauthentication configuration mode. To disable AAA bypass, use the **no** form of this command.

filter voice

no filter voice

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples The following example specifies that voice calls bypass AAA preauthentication:

```
Router(config)# aaa preauth
Router(config-preauth)# filter voice
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

flush

To enable file mode accounting flush options, use the **flush** command in privileged EXEC mode.

flush {**with-close** | **without-close**}

Syntax Description

with-close	Enables file accounting flush pending accounting to the file, and closes the file when the process is complete.
without-close	Enables file accounting flush pending accounting to file.

Command Default File mode accounting flush options are not enabled.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines The **flush** command flushes pending accounting records to the file.

Examples In the following example, the **flush with-close** command enables file accounting flush pending accounting to the file, and closes the file when the process is complete:

```
Router# flush with-close
```

Related Commands

Command	Description
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.

fmtp

To set a format-specific string for a codec, use the **fmtp** command in codec-profile configuration mode. To disable the format string, use the **no** form of this command.

fmtp *string*

no fmtp

Syntax Description

string	fmtp:payload type name1= val1; name2 = val2...

For Cisco Unified Customer Voice Portal (Cisco Unified CVP), the dynamic payload number is in the range of 96 to 127 for H.263+. For H263, it is always 34. For H.263+, this number must be entered but it is not used. Cisco Unified CVP uses either the default value for H.263+ (118) or the value defined for the VoIP dial peer using the command **rtp payload-type cisco-codec-video-h263+,** a number in the range 96 to 127.

Other parameters can be the following:

- SQCIF = 1 - 32
- QCIF = 1 - 32
- CIF = 1 - 32
- 4CIF = 1 - 32
- 16CIF = 1 - 32
- MAXBR (max bitrate) = Value in 100 bits per second (500 = 50000 bits per second). This value is another that is not used. Always set H.324 to 50K.
- D—1 (Enable H.263 Annex D)
- F—1 (Enable H.263 Annex F)
- I—1 (Enable H.263 Annex I)
- J—1 (Enable H.263 Annex J)
- K—1 to 4 (Enable H.263 Annex K) (Annex K is Slice Structured Mode)
  - 1—Slices In Order, Nonrectangular
  - 2—Slices In Order, Rectangular
  - 3—Slices Not Ordered, Nonrectangular
  - 4—Slices Not Ordered, Rectangular
- N=[1,4] (Enable H.263 Annex N) (Annex N is Reference Picture Selection Mode)
  - 1—NEITHER: No back-channel data is returned from the decoder to the encoder.
  - 2—ACK: The decoder returns only acknowledgment messages.
  - 3—NACK: The decoder returns only nonacknowledgment messages.
  - 4—ACK+NACK: The decoder returns both acknowledgment and nonacknowledgment messages.

- P=[x,y] (Enable H.263 Annex P) (Annex P is Reference Picture Resampling). Annex P can have either one or two parameters, depending on the values selected. There are four options, and six valid combinations.
  - 1—dynamicPictureResizingByFour
  - 2—dynamicPictureResizingBySixteenthPel
  - 3—dynamicWarpingHalfPel
  - 4—dynamicWarpingSixteenthPel.

  The valid combinations are:
  - 1
  - 1,3
  - 2
  - 2, 3
  - 2, 4
  - 3
- T=1 (Enable H.263 Annex T)
- CUSTOM = x, y, MPI — Defines a custom picture format, where X is the X-axis size in pixels, Y is the Y-axis size in pixels, and MPI is the frame rate (30/(1.001*MPI)). X and Y must be divisible by 4, and MPI has a value of 1to 32.

Command Default No string is configured.

Command Modes Codec-profile configuration (config-codec-profile)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines The profile is selected by entering the command:

video codec h263/h263+ profile 1000

The video codec h263/h263+ profile can be used in a voip dial peer or as a voice class codec entry.

Examples The following example shows an fmtp string for video codec profile 116:

```
codec profile 116 H263
    clockrate 90000
    fmtp "fmtp:120 SQCIF=1;QCIF=1;CIF=1;CIF4=2;MAXBR=3840;I=1"
```

Related Commands

Command	Description
clock-rate	Sets the clock rate for the codec.

forward-alarms

To turn on alarm forwarding so that alarms that arrive on one T1/E1 port are sent to the other port on dual-mode multiflex trunk interface cards, use the **forward-alarms** command in controller configuration mode on the one port. To reset to the default so that no alarms are forwarded, use the **no** form of this command.

forward-alarms

no forward-alarms

Syntax Description

This command has no arguments or keywords.

Command Default

Alarm forwarding is disabled

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

When you enter this command, physical-layer alarms on the configured port are forwarded to the other port on dual-port cards, simulating a one-way repeater operations. The system forwards RAIs (remote alarm indications, or Yellow Alarms), alarm indication signals (AIS, or Blue Alarms), losses of frame (LOF alarms, or Red Alarms), and losses of signaling (LOS alarms, or Red Alarms).

Examples

The following example turns on alarm forwarding on controller E1 0/0:

```
controller e1 0/0
 forward-alarms
```

forward-digits

To specify which digits to forward for voice calls, use the **forward-digits** command in dial peer configuration mode. To specify that any digits not matching the destination-pattern are not to be forwarded, use the **no** form of this command. To reset to the default, use the **default** form of this command.

forward-digits {*num-digit* | **all** | **extra**}

no forward-digits

default forward-digits

Syntax Description

num-digit	The number of digits to be forwarded. If the number of digits is greater than the length of a destination phone number, the length of the destination number is used. Range is 0 to 32. Setting the value to 0 is equivalent to entering the **no forward-digits** command.
all	Forwards all digits. If **all** is entered, the full length of the destination pattern is used.
extra	If the length of the dialed digit string is greater than the length of the dial-peer destination pattern, the extra right-justified digits are forwarded. However, if the dial-peer destination pattern is variable length ending with the character "T" (for example: T, 123T, 123...T), extra digits are not forwarded.

Command Default Dialed digits not matching the destination pattern are forwarded

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T. The **implicit** option was added.
12.0(4)T	This command was modified to support ISDNBF PRI QSIG signaling calls.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series. The **implicit** keyword was removed and the **extra** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines This command applies only to POTS dial peers. Forwarded digits are always right justified so that extra leading digits are stripped. The destination pattern includes both explicit digits and wildcards if present. Use the **default** form of this command if a nondefault digit-forwarding scheme was entered previously and you wish to restore the default.

For QSIG ISDN connections, entering the **forward-digits all** command implies that all the digits of the called party number are sent to the ISDN connection. When the **forward-digits** *num-digit* command and a number from 1 to 32 are entered, the number of digits of the called party number specified (right justified) are sent to the ISDN connection.

Examples

The following example shows that all digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 8...
 forward-digits all
```

The following example shows that four of the digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits 4
```

The following example shows that the extra right-justified digits that exceed the length of the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits extra
```

Related Commands

Command	Description
destination-pattern	Defines the prefix or the full E.164 telephone number to be used for a dial peer.
show dial-peer voice	Displays configuration information for dial peers.

frame-relay voice bandwidth

To specify how much bandwidth should be reserved for voice traffic on a specific data-link connection identifier (DLCI), use the **frame-relay voice bandwidth** command in map-class configuration mode. To release the bandwidth previously reserved for voice traffic, use the **no** form of this command.

frame-relay voice bandwidth *bps-reserved*

no frame-relay voice bandwidth *bps-reserved*

Syntax Description

bps-reserved	Bandwidth, in bits per second (bps), reserved for voice traffic for the specified map class. Range is from 8000 to 45000000. Default is 0, which disables voice calls.

Command Default Disabled (zero)

Command Modes Map-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(5)T	The **queue** *depth* keyword and argument were added.
12.2(1)	The **queue** *depth* keyword and argument were removed.

Usage Guidelines To use this command, you must first associate a Frame Relay map class with a specific DLCI and then enter map-class configuration mode and set the amount of bandwidth to be reserved for voice traffic for that map class.

If a call is attempted and there is not enough remaining bandwidth reserved for voice to handle the additional call, the call is rejected. For example, if 64 kbps is reserved for voice traffic and a codec and payload size is being used that requires 10 kbps of bandwidth for each call, the first six calls attempted are accepted, but the seventh call is rejected.

Reserve queues are not required for Voice over Frame Relay (VoFR).

Note Cisco strongly recommends that you set voice bandwidth to a value less than the committed information rate (CIR) if Frame Relay traffic shaping is configured. Cisco also strongly recommends that you set the minimum CIR (using the **frame-relay mincir** command) to be at least equal to or greater than the voice bandwidth.

Calculating Required Bandwidth

The bandwidth required for a voice call depends on the bandwidth of the codec, the voice packetization overhead, and the voice frame payload size. The smaller the voice frame payload size, the higher the bandwidth required for the call. To make the calculation, use the following formula:

required_bandwidth = codec_bandwidth x (1 + overhead / payload_size)

As an example, the overhead for a VoFR voice packet is between 6 and 8 bytes: a 2-byte Frame Relay header, a 1- or 2-byte FRF.11 header (depending on the CID value), a 2-byte cyclic redundancy check (CRC), and a 1-byte trailing flag. If voice sequence numbers are enabled in the voice packets, there is an additional 1-byte sequence number. Table 25 shows the required voice bandwidth for the G.729 8000-bps speech coder for various payload sizes.

Table 25 Required Voice Bandwidth Calculations for G.729

Codec	Codec Bandwidth	Voice Frame Payload Size	Required Bandwidth per Call (6-Byte OH)	Required Bandwidth per Call (8-Byte OH)
G.729	8000 bps	120 bytes	8400 bps	8534 bps
G.729	8000 bps	80 bytes	8600 bps	8800 bps
G.729	8000 bps	40 bytes	9200 bps	9600 bps
G.729	8000 bps	30 bytes	9600 bps	10134 bps
G.729	8000 bps	20 bytes	10400 bps	11200 bps

To configure the payload size for the voice frames, use the **codec** command from dial peer configuration mode.

Examples

The following example shows how to reserve 64 kbps for voice traffic for the “vofr” Frame Relay map class:

```
interface serial 1/1
 frame-relay interface-dlci 100
  class vofr
  exit
map-class frame-relay vofr
 frame-relay voice bandwidth 64000
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
frame-relay fair-queue	Enables weighted fair queueing for one or more Frame Relay PVCs.
frame-relay fragment	Enables fragmentation for a Frame Relay map class.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay mincir	Assigns the minimum CIR for Frame Relay traffic shaping.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

freq-max-delay

To specify the maximum timing difference allowed between the two frequencies for detection of a tone, use the **freq-max-delay** command **in** voice-class configuration mode. To reset to the default allowed timing difference, use the **no** form of this command.

freq-max-delay *time*

no freq-max-delay

Syntax Description

time	Maximum number of 10-millisecond time intervals by which the two frequencies in a tone may differ from each other and be detected. Range is from 10 to 100 (100 milliseconds to 1 second). The Default is 10 (100 milliseconds).

Command Default

10 (100 milliseconds)

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a time value greater than the timing difference expected in the tone to be detected.

Examples

The following example configures a maximum timing difference of 200 milliseconds for voice class 100:

```
voice class dualtone 100
 freq-max-delay 20
```

The following example configures a maximum timing difference of 160 milliseconds for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-delay 1
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-max-deviation

To specify the maximum frequency deviation allowed in a tone, use the **freq-max-deviation command in** voice-class configuration mode. To reset to the default maximum frequency deviation, use the **no** form of this command.

freq-max-deviation *frequency*

no freq-max-deviation

Syntax Description

frequency	Maximum cycles per second (Hz) by which tone frequencies may deviate from the configured frequencies and be detected. The value applies to both frequencies of a dual tone. Range is from 10 to 125. The default is 10.

Command Default 10 Hz

Command Modes Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

Be sure that the frequency deviation is less than the smallest frequency difference between any two call-progress tones to prevent overlapping of detectable frequencies. If detectable frequencies overlap, one of the call-progress tones is not detected.

You must specify a time value greater than the expected frequency deviation in the tone to be detected.

Examples The following example configures a maximum frequency deviation of 20 Hz for voice class 100:

```
voice class dualtone 100
 freq-max-deviation 20
```

The following example configures a maximum frequency deviation of 20 Hz for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-deviation 20
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters to a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-max-power

To specify the upper limit of tone power allowed in a tone, use the **freq-max-power** command in voice-class configuration mode. To reset to the default maximum tone power, use the **no** form of this command.

freq-max-power *dBm0*

no freq-max-power

Syntax Description

dBm0	Upper limit of the tone power that is detected, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from 0 to 20. The default is 10. **Note** The range is expressed in the negative of the desired level. A configured value of 20, equals -20 dBmO.

Command Default

10 dBm0

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value greater than the expected maximum power of a tone to be detected.

Examples

The following example configures a maximum tone power of -20 dBm0 for voice class 100:

```
voice class dualtone 100
 freq-max-power 20
```

The following example configures a maximum tone power of -6 dBm0 for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-power 6
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters defined by the **voice class dualtone-detect-params** command to a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-min-power

To specify the lower limit of tone power allowed in a tone, use the **freq-min-power** command in voice-class configuration mode. To reset to the default minimum tone power, use the **no** form of this command.

freq-min-power *dBm0*

no freq-min-power

Syntax Description

dBm0	Lower limit of tone power that is detected, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from 10 to 35. The default is 30. **Note** The range is expressed in the negative of the desired level. A configured value of 20, equals -20 dBmO.

Command Default 30 dBm0

Command Modes Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value less than the expected minimum power of a tone to be detected.

Examples The following example configures a tone-power lower limit of -15 dBm0 for voice class 100:

```
voice class dualtone 100
 freq-min-power 15
```

The following example configures a tone-power lower limit of -25 dBm0 for voice class 70:

```
voice class dualtone-detect-params 70
 freq-min-power 25
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters to a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-pair

To specify the frequency components of a tone to be detected, use the **freq-pair command in** voice-class configuration mode. To cancel detection of a tone, use the **no** form of this command.

freq-pair *tone-id frequency-1 frequency-2*

no freq-pair *tone-id*

Syntax Description

tone-id	Tag identifier for a tone to be detected. Range is from 1 to 16. There is no default.
frequency-1	One frequency component of the tone to be detected, in Hz. Range is from 300 to 3600. There is no default.
frequency-2	A second frequency component of the tone to be detected, in Hz. Range is frm 300 to 3600, or you can specify 0. There is no default.

Command Default No tone is specified for detection

Command Modes Voice-class configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines To detect a tone with two frequency components (a dualtone), configure frequencies for *frequency-1* and *frequency-2*.

To detect a tone with only one frequency component, configure a frequency for *frequency-1* and enter 0 for *frequency-2*.

You can configure a router to detect up to 16 tones.

Examples The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz:

```
voice class dualtone 100
 freq-pair 1 480 2400
 exit
```

The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz and tone number 2 (tone-id 2) with frequency components of 560 Hz and 880 Hz:

```
voice class dualtone 50
 freq-pair 1 480 2400
 freq-pair 2 560 880
 exit
```

Related Commands

Command	Description
frag-pre-queuing	Specifies the maximum timing difference allowed between the two frequencies for detection of a tone.
freq-max-deviation	Specifies the maximum frequency deviation allowed in a tone.
freq-max-power	Specifies the upper limit of the tone power allowed in a tone.
freq-min-power	Specifies the lower limit of the tone power allowed in a tone.
freq-power-twist	Specifies the power difference allowed between the two frequencies of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-power-twist

To specify the power difference allowed between the two frequencies of a tone, use the **freq-power-twist command in** voice-class configuration mode. To reset to the default power difference allowed, use the **no** form of this command.

freq-power-twist *dBm0*

no freq-power-twist

Syntax Description

dBm0	Maximum power difference allowed between the two frequencies of a tone, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from 0 to 15. The default is 6.

Command Default

6 dBm0

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value greater than the expected maximum power difference of the two frequencies in the tone to be detected.

Examples

The following example configures a maximum allowed power difference of 3 dBm0 between the two tone frequencies for voice class 100:

```
voice class dualtone 100
 freq-power-twist 3
```

The following example configures a maximum allowed power difference of 15 dBm0 between the two tone frequencies in voice class 70:

```
voice class dualtone-detect-params 70
 freq-power-twist 15
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters defined by the **voice class dualtone-detect-params** command to a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

frequency (cp-dualtone)

To define the frequency components for a call-progress tone, use the **frequency** command in cp-dualtone configuration mode. To reset to the default frequency components, use the **no** form of this command.

frequency *frequency-1* [*frequency-2*]

no frequency

Syntax Description

frequency-1	One frequency component of the tone to be detected, in Hz. Range is from 300 to 3600. The default is 300.
frequency-2	(Optional) A second frequency component of the tone to be detected, in Hz. Range is from 300 to 3600 or you can specify 0. The default is that no second frequency component is detected.

Command Default 300-Hz single tone

Command Modes cp-dualtone configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines This command specifies the frequency component for a class of custom call-progress tones.

You need to define the frequency that you want a voice port to detect. Reenter the command for each additional frequency to be detected.

You need to associate the class of custom call-progress tones with a voice port for this command to affect tone detection.

Examples The following example defines the frequency components for the busy tone in custom-cptone voice class country-x.

```
voice class custom-cptone country-x
 dualtone busy frequency 480 620
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the boundaries and limits for custom call-progress tones defined by the **voice class custom-cptone** command.

Cisco IOS Voice Commands: G

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

g729 annexb-all

To configure Cisco IOS Session Initiation Protocol (SIP) gateway to treat the G.729br8 codec as superset of G.729r8 and G.729br8 codecs to interoperate with the Cisco Unified Communications Manager, use the **g729 annexb-all** command in voice service SIP configuration mode. To return to the default global setting for the gateway, where G.729br8 codec represents only the G.729br8 codec, use the **no** form of this command.

g729 annexb-all

no g729 annexb-all

Syntax Description

annexb-all	Specifies that the G.729br8 codec is treated as a superset of G.729r8 and G.729br8 codecs to communicate with Cisco Unified Communications Manager.

Command Default

G.729br8 codec is not viewed as superset of G.729r8 and G.729br8 codecs.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

There are four variations of the G.729 coder-decoder (codec), which fall into two categories:

High Complexity

- G.729 (g729r8)—a high complexity algorithm codec on which all other G.729 codec variations are based.
- G.729 Annex-B (g729br8 or G.729B)—a variation of the G.729 codec that allows the DSP to detect and measure voice activity and convey suppressed noise levels for re-creation at the other end. Additionally, the Annex-B codec includes Internet Engineering Task Force (IETF) voice activity detection (VAD) and comfort noise generation (CNG) functionality.

Medium Complexity

- G.729 Annex-A (g729ar8 or G.729A)—a variation of the G.729 codec that sacrifices some voice quality to lessen the load on the DSP. All platforms that support G.729 also support G.729A.
- G.729A Annex-B (g729abr8 or G.729AB)—a variation of the G.729 Annex-B codec that, like G.729B, sacrifices voice quality to lessen the load on the DSP. Additionally, the G.729AB codec also includes IETF VAD and CNG functionality.

The VAD and CNG functionality is what causes the instability during communication attempts between two DSPs where one DSP is configured with Annex-B (G.729B or G.729AB) and the other without (G.729 or G.729A). All other combinations interoperate. To configure a Cisco IOS SIP gateway for

interoperation with Cisco Unified Communications Manager (formerly known as the Cisco CallManager, or CCM), use the **g729-annexb-all** command in voice service SIP configuration mode to allow connection of calls between two DSPs with incompatible G.729 codecs. Use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode to configure G.729 codec interoperation settings for a dial peer that override global settings for the Cisco IOS SIP gateway.

Examples

The following example configures a Cisco IOS SIP gateway (globally) to be able to connect calls between otherwise incompatible G.729 codecs:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# g729 annexb-all
```

Related Commands

Command	Description
voice-class sip g729 annexb-all	Configures an individual dial peer on a Cisco IOS SIP gateway to view a G.729br8 codec as superset of G.729r8 and G.729br8 codecs.

g732 ber

To enable G.732 processing and reporting for the E1 controller, use the **g732 ber** command in controller configuration mode. To disable processing and reporting, use the **no** form of this command.

g732 ber

no g732 ber

Syntax Description

This command has no arguments or keywords.

Command Default

G.732 is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 2611.
12.2(15)T	This command was implemented on the Cisco AS5350 and Cisco AS5400 network access server (NAS) platforms.

Usage Guidelines

By default, G.732 reporting is disabled to prevent a change in E1 behavior for sites that do not want G.732 reporting.

Once ITU-T G.732 is enabled, the E1 controller is placed in the DOWN state if the bit error rate (BER) on the line is greater than 10e-3. The controller is restored to the UP state if the BER drops below 10e-4 for longer than two seconds. When the G.732 alarm is declared, the transmitter sends a remote alarm indication (RAI) yellow alarm.

You can restore ITU-T G.732 functionality by performing a power cycle or a software reload.

Examples

The following example applies to a Cisco 2611 and shows enabled G.732 processing and reporting for E1 controller 0/0:

```
controller e1 0/0
 g732 ber
```

The following example applies to a Cisco AS5400 with an 8-PRI E1 dial feature card (DFC) in slot 4:

```
controller e1 4/0
 g732 ber
```

Related Commands

Command	Description
show controllers e1	Displays information about E1 links.

gatekeeper

To enter gatekeeper configuration mode, use the **gatekeeper** command in global configuration mode.

gatekeeper

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines Press **Ctrl-Z** or use the **exit** command to exit gatekeeper configuration mode.

Examples The following example brings the gatekeeper online:

```
gatekeeper
 no shutdown
```

gateway

To enable the H.323 VoIP gateway, use the **gateway** command in global configuration mode. To disable the gateway, use the **no** form of this command.

gateway

no gateway

Syntax Description This command has no arguments or keywords.

Command Default The gateway is unregistered

Command Modes Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 3600 series, Cisco AS5300, and Cisco AS5800.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines Use this command to enable H.323 VoIP gateway functionality. After you enable the gateway, it attempts to discover a gatekeeper by using the H.323 RAS GRQ message. If you enter **no gateway voip**, the VoIP gateway unregisters with the gatekeeper via the H.323 RAS URQ message.

Examples The following example enables the gateway:

```
gateway
```

gcid

To enable Global Call ID (Gcid) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint, use the **gcid** command in voice-service configuration mode. To return to the default, use the **no** form of this command.

gcid

no gcid

Syntax Description

This command has no arguments or keywords.

Command Default

Gcid is disabled.

Command Modes

Voice-service configuration (config-voi-serve)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(11)XW2	Cisco Unified CME 4.2	This command was introduced.
12.4(15)XY	Cisco Unified CME 4.2 (1)	This command was introduced.
12.4(15)XZ	Cisco Unified CME 4.3	This command was introduced.
12.4(20)T	—	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command in voice-service configuration mode enables Global Call ID (Gcid) in the SIP header for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.

When a call moves around and between the SIP endpoint and the target on a VoIP network because of redirect, transfer, and conference, the SIP Call-ID continues to change. For call control purposes, a unique Gcid is issued for every outbound call leg. A single Gcid remains the same for the same call in the system, and is valid for redirect, transfer, and conference events, including 3-party conferencing when a call center phone acts as a conference host. A SIP header, Cisco_GCID, is added into SIP Invite and REFER requests and to certain other responses to pass the Gcid to the target.

Examples

The following partial output shows the configuration for the **gcid** command:

```
router# show running-configuration
!
!
!
voice service voip
 gcid
 callmonitor
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 sip
 registrar server expires max 120 min 60
```

global (application configuration)

To enter application configuration global mode, use the **global** command in application configuration mode.

global

Syntax Description No arguments or keywords

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to enter application configuration global mode. You can then configure applications for a dial peer to use for incoming calls when it does not have an explicit application configured.

If an application is defined on the dial peer, that application always takes precedence over the global application configured in application configuration global mode. The applications configured in this mode execute only when a dial peer has no application configured.

Examples The following example shows the clid_authen_collect application is configured as the default global application for all inbound dial peers that do not have a specific application configured:

```
application
    global
    service default clid_authen_collect
```

Related Commands

Command	Description
call application global	Configures an application to use for incoming calls whose incoming dial peer does not have an explicit application configured.

groundstart auto-tip

To configure a timing delay on an FXO groundstart voice port, use the **groundstart auto-tip** command in voice-port configuration mode. To disable the configured timeout, use the **no** form of this command.

groundstart auto-tip [**delay** *timer*]

no groundstart auto-tip [**delay** *timer*]

Syntax Description

delay	Indicates that a specific delay time will be configured.
timer	Specifies the wait time in milliseconds that the FXO groundstart voice port will wait for a tip ground acknowledgment.

Command Default

This command is disabled by default. If the command is used without the optional keyword, the default time of 200 ms is activated.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(11)T2	This command was introduced into Cisco IOS Release 12.3(11)T2. This command is not supported on the Cisco 1700 series platform.

Usage Guidelines

This command should only be used after you encounter call setup problems involving FXO groundstart analog voice ports. If these problems occur, first load the latest image for your Cisco IOS Release (for example, if you are running Release 12.3(11)T, you should replace this image with Release 12.3(11)T2. Upgrading the software image should eliminate the problem. If not, then use this command as a troubleshooting measure—it should be enabled in a configuration only if you encounter problems in connecting outgoing calls. After the **groundstart auto-tip** command is configured, the problem should not occur again.

Use the **groundstart auto-tip** command only for voice ports configured for FXO groundstart signaling.

The following example sets the delay wait time for tip ground acknowledgment to 250 ms:

```
Router# configure terminal
Router(config)# voice-port 2/0/0
Router(config-voiceport)# shutdown
Router(config-voiceport)# groundstart auto-tip delay 250
Router(config-voiceport)# no shutdown
Router(config-voiceport)# exit
```

Related Commands

Command	Description
voice-port	Specifies that a voice port will be used in the connection.

group

To configure the maximum number of segments that are received in a session group or to associate the group with a specified session set, use the **group** command in backhaul-session-manager configuration mode. To restore the default number, use the **no** form of this command.

group {*group-name* **cumulative ack** *count* | **out-of-sequence** *count* | **receive** *count* | **retransmit** *count* | **set** *set-name*}

no group {*group-name* **cumulative ack** | **out-of-sequence** | **receive** | **retransmit** | **set**}

Caution Do not change this command or the keywords unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

group-name	Session-group name.
cumulative ack *count*	Maximum number of segments received before acknowledgment. Range is from 0 to 255. Default is 3 segments.
out-of-sequence *count*	Maximum number of out-of-sequence segments that can be received in a session group before an ACK is sent. Range is from 0 to 255. Default is 3 segments.
receive *count*	Maximum number of segments in the receive window of the media gateway. This is the maximum number of segments the media gateway is allowed to receive before it sends an ACK. Range is from 1 to 64. Default is 32 segments.
retransmit *count*	Maximum number of retransmits allowed in a session group. Range is from 0 to 255. Default is 2 retransmits.
set *set-name*	Session-set name.

Command Default

For the **cumulative ack** and **out-of-sequenc**e keywords, the default is 3 segments.
For the **receive** keyword, the default is 32 segments.
For the **retransmit** keyword, the default is 2 retransmits.
The **set** keyword has no default behavior or values.

Command Modes

Backhaul-session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command was implemented on the Cisco IAD2420 series. This command does not support the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example configures the session group named group5 to send an acknowledgment after four segments have been received:

```
group group5 cumulative-ack 4
```

The following example configures the session group named group5 to send an acknowledgment after four out-of-sequence segments have been received:

```
group group5 out-of-sequence 4
```

The following example configures the session group named group5 to receive a maximum of 10 segments:

```
group group5 receive 10
```

The following example configures the session group named group5 to allow as many as 3 retransmits:

```
group group5 retransmit 3
```

The following example associates the session group named group5 with the session set named set1:

```
group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Specifies maximum cumulative acknowledgments.
group out-of-sequence	Specifies maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Specifies maximum receive segments.
group retransmit	Specifies maximum retransmits.
group timer	Specifies timeouts.

group auto-reset

To specify the maximum number of auto-resets for a session group, use the **group auto-reset** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *group-name* **auto-reset** *count*

no group *group-name* **auto-reset**

Caution Do not change the auto-reset number unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

group-name	Name of session group.
count	Maximum number of auto-resets before the connection is considered failed. Range is from 0 to 255. The default is 5.

Command Default

5 auto-resets

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example specifies a maximum of six auto-resets for the session group named “group5”:

```
Router(config-bsm)# group group5 auto-reset 6
```

Related Commands

Command	Description
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.

group cumulative-ack

To configure the maximum number of segments that are received before an acknowledgment is sent, use the **group cumulative-ack** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **cumulative-ack** *count*

no group *group-name* **cumulative-ack** *count*

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Syntax Description

group-name	Name of session group.
count	Maximum number of segments that are received before acknowledgment. Range is from 0 to 255. The default is 3.

Command Default

3 segments

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example sets the cumulative acknowledgment maximum to 4 for the group named "group1":

```
Router(config-bsm)# group group5 cumulative-ack 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.

group receive	Configures the maximum number of receive segments.
group retransmit	Configures the maximum number of retransmits.

group out-of-sequence

To configure the maximum number of out-of-sequence segments that are received before an error acknowledgement (EACK) is sent, use the **group out-of-sequence** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **out-of-sequence** *count*

no group *group-name* **out-of-sequence** *count*

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Syntax Description

group-name	Name of the session group.
count	Maximum number of out-of-sequence segments. Range is from 0 to 255. The default is 3.

Command Default

3 segments

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example sets the out-of-sequence maximum to 4 for the group named “group5”:

```
Router(config-bsm)# group group5 out-of-sequence 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.
group receive	Configures the maximum number of receive segments.
group retransmit	Configures the maximum number of retransmits.

group receive

To configure the maximum number of receive segments, use the **group receive** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **receive** *count*

no group *group-name* **receive** *count*

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Syntax Description

group-name	Name of the session group.
count	Maximum number of segments in a receive window. The far end should send no more than this number of segments before receiving an acknowledgment for the oldest outstanding segment. Range is 1 to 64. The default is 32.

Command Default 32 segments

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples The following example sets the receive maximum to 10 for the group named “group5”:

```
Router(config-bsm)# group group5 receive 10
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.

group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.
group retransmit	Configures the maximum number of retransmits.

group retransmit

To configure the maximum number of retransmits, use the **group retransmit** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **retransmit** *count*

no group *group-name* **retransmit** *count*

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Syntax Description

group-name	Name of the session group.
count	Maximum number of retransmits. Range is 0 to 255. The default is 2.

Command Default 2 retransmits

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples The following example sets the retransmit maximum to 3 for the group named “group5”:

```
Router(config-bsm)# group group5 retrans 3
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of receive segments.

group set

To create a session group and associate it with a specified session set, use the **group** command in backhaul session manager configuration mode. To delete the group, use the **no** form of this command.

group *grp-name* **set** *set-name*

no group *grp-name*

Syntax Description

grp-name	Name of the session group.
set-name	Name of the session set.

Command Default No default behavior or values

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series.

Examples The following example shows session group **group5** being associated with session set **set1**:

```
Router(config-bsm)# group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.

Command	Description
group timer transfer	Configures state transfer timeout.
group auto-reset	Specifies the maximum number of auto-resets for a session group.

group timer

To configure the maximum number of milliseconds for which the Reliable User Datagram Protocol (RUDP) delays before sending an acknowledgment for a received segment, sending a keepalive segment, retransmitting a segment, or transferring a segment, use the **group timer** command in backhaul-session-manager configuration mode. To restore the default values, use the **no** form of this command.

group *group-name* **timer** {**cumulative ack** *time* | **keepalive** *time* | **retransmit** *time* | **transfer** *time*}

no group *group-name* **timer** {**cumulative ack**}

Caution Do not change the group timer parameters unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

group-name	Name of session group.
cumulative ack *time*	Number of milliseconds for which RUDP delays before sending an acknowledgment for a received segment. Range is 100 to 65535. The default is 100.
keepalive *time*	Number of milliseconds before RUDP sends a keepalive segment when no RUDP packets are received or sent. Range is 100 to 65535. The default is 1000.
retransmit *time*	Number of milliseconds for which RUDP waits before retransmitting the segment. Range is 100 to 65535. The default is 300.
transfer *time*	Number of milliseconds for which RUDP waits to receive a selection of a new session from the application during a transfer state. Range is 0 to 65535. The default is 2000.

Command Default

cumulative ack: 100 milliseconds
keepalive: 1000 milliseconds
retransmit: 300 milliseconds
transfer: 2000 milliseconds

Command Modes

Backhaul-session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

The retransmit timer must be greater than the cumulative-ack timer.

Cumulative acknowledgment timeout is the maximum number of milliseconds for which RUDP delays before sending an acknowledgment for a received segment.

Examples

The following example specifies 325 milliseconds as the maximum acknowledgment delay for the session group named “group5”:

```
group group5 timer cumulative-ack 325
```

The following example configures RUDP to send keepalive segments if no RUDP packets are received or sent for 2.5 seconds (2500 milliseconds) in the session group named “group5”.

```
group group5 timer keepalive 2500
```

The following example sets a retransmit time of 650 milliseconds for the session group named “group5”:

```
group group5 timer retransmit 650
```

Related Commands

Command	Description
group	Specifies the maximum number of segments that are received in a session group.

group-params

To define groups of parameters that can be used by applications, use the **group-params** command in application configuration mode.

group-params *groupname*

Syntax Description

groupname	Name of the parameter group you are creating.

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command allows you to define groups of parameters so that a group of parameters can be used by multiple services or packages (applications). Parameter groups are defined globally and once a group is defined, it is available for another service or package to use. Groups can contain parameters under multiple parameterspaces. In cases where a parameter is defined individually and in a parameter group, the individual parameter definition is given precedence.

Examples

The following example shows a parameter group named “fax,” that contains two parameters:

```
application
group-params fax
  paramspace fax_detect2 pin-len 9
  paramspace fax_detect1 retry-count 9
```

gw-accounting

To enable an accounting method for collecting call detail records (CDRs), use the **gw-accounting** command in global configuration mode. To disable an accounting method, use the **no** form of this command.

gw-accounting {**aaa** | **file** | **syslog** [**stats**] }

no gw-accounting {**aaa** | **file** | **syslog** [**stats**] }

Cisco IOS Release 12.2(8)T and Earlier Releases

gw-accounting {**h323** [**vsa**] | **syslog** | **voip**}

no gw-accounting {**h323** [**vsa**] | **syslog** | **voip**}

Syntax Description

aaa	Enables accounting through the AAA system and sends call detail records to the RADIUS server in the form of vendor-specific attributes (VSAs).
file	Enables the file accounting method to store call detail records in .csv format.
syslog	Enables the system logging facility to output accounting information in the form of a system log message.
stats	(Optional) Enables voice quality statistics to be sent to the system log.
h323	Enables standard H.323 accounting using Internet Engineering Task Force (IETF) RADIUS attributes.
vsa	(Optional) Enables H.323 accounting using RADIUS VSAs.
voip	Enables generic gateway-specific accounting.

Command Default

No accounting method is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T. The **vsa** keyword was added.
12.1(1)T	The **voip** keyword was added.
12.2(11)T	The **h323**, **vsa**, and **voip** keywords were replaced by the **aaa** keyword.
12.4(11)XW	The **stats** keyword was added.
12.4(15)XY	The **file** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command enables you to output accounting data in one of the following ways:

Using RADIUS Vendor-Specific Attributes

The IETF draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not appropriate for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the format:

```
protocol: attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS. For a list of VSA fields and their ASCII values, see the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.

Use the **gw-accounting aaa** command to enable the VSA method of accounting.

Note Releases earlier than Cisco IOS Release 12.2(11)T use the **gw-accounting h323 vsa** command.

Using File Format

This method stores CDRs in comma separated values (CSV) format. These CDR records can be stored in a file on external or internal flash or on a file on a FTP server.

Each CDR has a fixed number of fields whose names and position order are predefined. Ten generic fields capture feature-related information. The CDR has feature fields representing the basic feature and feature fields representing the supplementary services.

Use the **gw-accounting file** command to enable the .csv file method of accounting.

Using syslog Records

The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

Use the **gw-accounting syslog** command to enable the syslog method of gathering accounting data.

Table 26 describes the syslog message fields.

Table 26 syslog Message Output Fields

Field	Description
server timestamp	Time stamp created by the server when it receives the message to log.
gateway id	Name of the gateway that sends the message.
message number	Number assigned to the message by the gateway.
message label	String used to identify the message category.
list of AV pairs	String that consists of <attribute name> <attribute value> pairs separated by commas.

You can enable **aaa**, **file**, or **syslog** simultaneously; call detail records are generated using all methods that you enable.

Overloading the Acct-Session-ID field

Attributes that cannot be mapped to standard RADIUS are packed into the Acct-Session-ID field as ASCII strings separated by the character "/". The Acct-Session-ID attribute definition contains the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, the following string format is defined for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

Table 27 describes the field attributes that are used with the overloaded acct-session-ID method.

Table 27 Field Attributes in Overloaded Acct-Session-ID

Field Attribute	Description
Session-Id	Standard RADIUS account session ID.
Setup-Time	Q.931 setup time for this connection in Network Time Protocol (NTP) format: hour, minutes, seconds, milliseconds, time zone, day of week, month, day of month, and year.
Gateway-Id	Name of the underlying gateway in the form "gateway.domain_name."
Call-Origin	Origin of the call relative to the gateway. Possible values are **originate** and **answer**.
Call-Type	Call leg type. Possible values are **telephony** and **VoIP**.
Connection-Id	Unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word displays as a hexadecimal value separated by a space character.
Connect-Time	Q.931 connect time for this call leg, in NTP format.
Disconnect-Time	Q.931 disconnect time for this call leg, in NTP format.
Disconnect-Cause	Reason that a call was taken offline as defined in the Q.931 specification.
Remote-Ip-Address	Address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-ID string, it is impossible to include many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **attribute acct-session-id overloaded** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

Note Releases earlier than Cisco IOS Release 12.2(11)T use the **gw-accounting h323** command.

Examples

The following example shows accounting enabled using RADIUS VSA attributes:

```
gw-accounting aaa
```

The following example shows accounting enabled using the syslog method:

```
gw-accounting syslog
```

The following example shows accounting enabled using the file method:

```
gw-accounting file
```

Related Commands

Command	Description
acct-template	Selects a group of voice accounting attributes to collect.
attribute acct-session-id overloaded	Overloads the acct-session-id attribute with call detail records.
radius-server vsa send	Enables the voice gateway to recognize and use VSAs.

gw-type-prefix

To configure a technology prefix in the gatekeeper, use the **gw-type-prefix** command in gatekeeper configuration mode. To remove the technology prefix, use the **no** form of this command.

gw-type-prefix *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq | blast**]] [**default-technology**] [[**gw ipaddr** *ipaddr* [*port*]]]

no gw-type-prefix *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq | blast**]] [**default-technology**] [[**gw ipaddr** *ipaddr* [*port*]]]

Syntax Description

type-prefix	A technology prefix is recognized and is stripped before checking for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#.
hopoff *gkid*	(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The *gkid* argument refers to a gatekeeper previously configured using the zone local or zone remote comment. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix.
seq | blast	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which they were listed. The default is to send them sequentially.
default-technology	(Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved.
gw ipaddr *ipaddr* [*port*]	(Optional) Use this option to indicate that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.

Command Default

By default, no technology prefix is defined, and LRQs are sent sequentially to all the gatekeepers listed.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. This command was modified to allow the user to specify multiple hopoffs.
12.1(2)T	This command was modified to allow the user to specify whether LRQs should be sent simultaneously or sequentially to the gatekeepers.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco MC3810, and Cisco 7200 series.

Usage Guidelines

More than one gateway can register with the same technology prefix. In such cases, a random selection is made of one of them.

You do not have to define a technology prefix to a gatekeeper if there are gateways configured to register with that prefix and if there are no special flags (**hopoff** *gkid* or **default-technology**) that you want to associate with that prefix.

You need to configure the gateway type prefix of all remote technology prefixes that are routed through this gatekeeper.

Examples

The following example defines two gatekeepers for technology zone 3:

```
gw-type-prefix 3#* hopoff c2600-1-gk hopoff c2514-1-gk
```

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the list of currently defined technology zones and the gatekeepers responsible for each.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.

Cisco IOS Voice Commands: H

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command referenefces. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

h225 alt-ep hunt

To configure alternate endpoint hunts for failed calls in an IP-to-IP gateway (IPIPGW), use the **h225 alt-ep hunt** command in H.323 voice-service configuration mode. To control the alternate endpoint hunts based on call disconnect cause codes, use the **no** form of this command.

h225 alt-ep hunt

no h225 alt-ep hunt [**all** | *cause-code*]

Syntax Description

all	Perform alternate hunt for all disconnect cause codes.
cause-code	A code returned from the destination router to indicate why an attempted end-to-end call was unsuccessful. Table 28 in the "Usage Guidelines" section describes the possible values.

Command Default

Alternate endpoint hunt is enabled for all cause codes

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The default behavior of the gateway is to retry all alternate endpoints received from the gatekeeper regardless of the ReasonComplete reason. Only the **no alt-ep hunt** command will be visible in the configuration. A code returned from the destination router to indicate why an attempted end-to-end call was unsuccessful. If the specified disconnect cause code is returned from the last destination endpoint, dial peer hunting is enabled or disabled. You can enter the keyword, decimal value, or hexadecimal value.

The disconnect cause codes are described in Table 28. The decimal and hexadecimal value of the disconnect cause code follows the description of each possible keyword.

Table 28 Standard Disconnect Cause Codes

Keyword	Description	Decimal	Hex
access-info-discard	Access information discarded.	43	0x2b
all	Continue dial-peer hunting for all disconnect cause codes received from a destination router.		
b-cap-not-implemented	Bearer capability not implemented.	65	0x41
b-cap-restrict	Restricted digital information bearer capability only.	70	0x46
b-cap-unauthorized	Bearer capability not authorized.	57	0x39

Table 28 Standard Disconnect Cause Codes (continued)

Keyword	Description	Decimal	Hex
b-cap-unavail	Bearer capability not available.	58	0x3a
call-awarded	Call awarded.	7	0x7
call-cid-in-use	Call exists, call ID in use.	83	0x53
call-clear	Call cleared.	86	0x56
call-reject	Call rejected.	21	0x15
cell-rate-unavail	Cell rate not available.	37	0x25
channel-unacceptable	Channel unacceptable.	6	0x6
chantype-not-implement	Channel type not implemented.	66	0x42
cid-in-use	Call ID in use.	84	0x54
codec-incompatible	Codec incompatible.	171	0xab
cug-incalls-bar	Closed user group (CUG) incoming calls barred.	55	0x37
cug-outcalls-bar	CUG outgoing calls barred.	53	0x35
dest-incompatible	Destination incompatible.	88	0x58
dest-out-of-order	Destination out of order.	27	0x1b
dest-unroutable	No route to destination.	3	0x3
dsp-error	Digital signal processor (DSP) error.	172	0xac
dtl-trans-not-node-id	Designated transit list (DTL) transit not my node ID.	160	0xa0
facility-not-implemented	Facility not implemented.	69	0x45
facility-not-subscribed	Facility not subscribed.	50	0x32
facility-reject	Facility rejected.	29	0x1d
glare	Glare.	15	0xf
glaring-switch-pri	Glaring switch primary rate ISDN (PRI).	180	0xb4
htspm-oos	Holst Telephony Service Provider Module (HTSPM) out of service.	129	0x81
ie-missing	Mandatory information element missing.	96	0x60
ie-not-implemented	Information element not implemented.	99	0x63
info-class-inconsistent	Inconsistency in information and class.	62	0x3e
interworking	Interworking.	127	0x7f
invalid-call-ref	Invalid call reference value.	81	0x51
invalid-ie	Invalid information element contents.	100	0x64
invalid-msg	Invalid message.	95	0x5f
invalid-number	Invalid number.	28	0x1c
invalid-transit-net	Invalid transit network.	91	0x5b
misdialled-trunk-prefix	Misdialed trunk prefix.	5	0x5
msg-incomp-call-state	Message in incomplete call state.	101	0x65
msg-not-implemented	Message type not implemented.	97	0x61

Table 28 Standard Disconnect Cause Codes (continued)

Keyword	Description	Decimal	Hex
msgtype-incompatible	Message type not compatible.	98	0x62
net-out-of-order	Network out of order.	38	0x26
next-node-unreachable	Next node unreachable.	128	0x80
no-answer	No user answer.	19	0x13
no-call-suspend	No call suspended.	85	0x55
no-channel	Channel does not exist.	82	0x52
no-circuit	No circuit.	34	0x22
no-cug	Nonexistent CUG.	90	0x5a
no-dsp-channel	No DSP channel.	170	0xaa
no-req-circuit	No requested circuit.	44	0x2c
no-resource	No resource.	47	0x2f
no-response	No user response.	18	0x12
no-voice-resources	No voice resources available.	126	0x7e
non-select-user-clear	Nonselected user clearing.	26	0x1a
normal-call-clear	Normal call clearing.	16	0x10
normal-unspecified	Normal, unspecified.	31	0x1f
not-in-cug	User not in CUG.	87	0x57
number-changeed	Number changed.	22	0x16
param-not-implemented	Nonimplemented parameter passed on.	103	0x67
perm-frame-mode-oos	Permanent frame mode out of service.	39	0x27
perm-frame-mode-oper	Permanent frame mode operational.	40	0x28
precedence-call-block	Precedence call blocked.	46	0x2e
preempt	Preemption.	8	0x8
preempt-reserved	Preemption reserved.	9	0x9
protocol-error	Protocol error.	111	0x6f
qos-unavail	QoS unavailable.	49	0x31
rec-timer-exp	Recovery on timer expiry.	102	0x66
redirect-to-new-destination	Redirect to new destination.	23	0x17
req-vpci-vci-unavail	Requested virtual path connection identifier (VPCI) virtual channel identifier (VCI) not available.	35	0x23
send-infotone	Send information tone.	4	0x4
serv-not-implemented	Service not implemented.	79	0x4f
serv/opt-unavail-unspecified	Service or option not available, unspecified.	63	0x3f
stat-enquiry-resp	Response to status inquiry.	30	0x1e
subscriber-absent	Subscriber absent.	20	0x14
switch-congestion	Switch congestion.	42	0x2a

Table 28 Standard Disconnect Cause Codes (continued)

Keyword	Description	Decimal	Hex
temp-fail	Temporary failure.	41	0x29
transit-net-unroutable	No route to transit network.	2	0x2
unassigned-number	Unassigned number.	1	0x1
unknown-param-msg-discard	Unrecognized parameter message discarded.	110	0x6e
unsupported-aal-parms	ATM adaptation layer (AAL) parameters not supported.	93	0x5d
user-busy	User busy.	17	0x11
vpci-vci-assign-fail	Virtual path connection identifier virtual channel identifier (VPCI VCI) assignment failure.	36	0x24
vpci-vci-unavail	No VPCI VCI available.	45	0x2d

Examples

The following example shows the alternate endpoint hunts with the user-busy disconnect cause code disabled:

```
Router(conf-serv-h323)# no h225 alt-ep hunt user-busy
```

Related Commands

Command	Description
gatekeeper	Enters gatekeeper configuration mode.

h225 connect-passthru

To immediately pass H.225 connect messages from the trunking gateway to the outgoing gateway via a Cisco Unified Border Element, use the **h225 connect-passthru** command in voice class or H.323 voice-service configuration mode. To return to the default behavior, use the **no** form of this command.

h225 connect-passthru

no h225 connect-passthru

Syntax Description

This command has no arguments or keywords.

Command Default

The H.225 messages are not sent to the outgoing gateway until TCS/MSD/OLC negotiation takes place.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Calls placed through a Cisco Unified Border Element may fail to connect when the originating or terminating H.323 device is a non-Cisco IOS VoIP device such as Cisco Unified Communications Manager.

The default behavior of H.323-to-H.323 calls through a Cisco Unified Border Element is to delay sending a H.225 Connect message to the originating H323 device until the H245 TCS/MSD/OLC negotiation takes place. During this process, an H.225 Connect message with an H.245 address present from the terminating H.323 device is changed to an H.225 Progress message, followed by an H.225 Facility message with the embedded H.245 address. This can cause connection failures if the originating H.323 device is waiting for the H.225 Connect message to begin the H245 TCS/MSD/OLC negotiation.

The **h225 connect-passthru** command is used to immediately pass H.225 connect messages from the trunking gateway to the outgoing gateway via a Cisco Unified Border Element.

Configuring the **h225 connect-passthru** command in H.323 voice-service configuration is recommended for all calls passed through the Cisco Unified Border Element. This command option will be present only when the **allow-connections** command is configured.

This command is often configured with the **h245 passthru tcsnonstd-passthru** command and **emptycapability** command when interworking is configured between non-Cisco IOS H.323 devices.

Examples

The following example shows the **h225 connect-passthru** command being configured under H.323 voice-service configuration mode:

```
Router(conf-serv-h323)# h225 connect-passthru
```

The following example shows the **h225 connect-passthru** command being configured under voice class configuration mode:

```
Router(config-class)# h225 connect-passthru
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
emptycapability	Eliminates the need for identical codec capabilities for all dial peers in the rotary group
h245 passthru tcsnonstd-passthru	Passes TCS parameter (CCM data only).

h225 display-ie

To allow the Cisco Unified Communication Manager to ignore the H.225 Facility message and process the H.225 Notify message used to display the calling name on the IP Phone, use the **h225 display-ie ccm-compatible** command in voice service or voice class configuration mode. To return to the default configuration, use the **no** version of the command.

h225 display-ie ccm-compatible system

no h225 display-ie ccm-compatible system

Syntax Description

ccm-compatible	Q931 Facility with calling name is received the gateway sends both H225 Notify and H225 Facility messages with the calling name in the Display IE.
system	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone

Command Default

Disabled. The Cisco Unified Communication Manager ignores the IE and does not display the calling name on the Cisco IP Phone.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12. 4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When the gateway is interoperating with Cisco Unified Communication Manager, you must enable the **h225 display-ie ccm-compatible** command to display the IE received in Q931 Facility message is sent out in the H.225 Notify message.

When the **h225 display-ie ccm-compatible** command is configured, the gateway sends the H.225 Facility message and the H.225 Notify message to the Cisco Unified Communication Manager, which ignores the H.225 Facility message, and processes the H.225 Notify message.

Note While interoperating only with Cisco Unified Connections Manager you must configure the **h225 display-ie ccm-compatible** command.

Behavior and configuration will vary based on the configuration mode the command is configured:

- When the **h225 display-ie ccm-compatible** command is configured under voice class, the CLI under voice class takes precedence. Even if the **h225 display-ie ccm-compatible** command is not configured under global voice service voip, the command configured under voice class takes effect. This means that when a Q931 Facility with calling name is received the gateway sends both H225 Notify and H225 Facility messages with the calling name in the Display IE.

The configured command is visible in the **show running-configuration** output under voice class.

- When the **h225 display-ie ccm-compatible system** command is configured under voice class, the command configured under global voice service VoIP takes precedence. If the **h225 display-ie ccm-compatible system** command is configured under voice service voip, the gateway sends a H225 Notify message. If the **h225 display-ie ccm-compatible system** command is not configured under voice service voip, the gateway will not send the H225 Notify message.

  When the **system** keyword is configured, the command is not visible in the **show running-configuration** output.

- Configuring **no h225 display-ie ccm-compatible system** in voice class configuration mode, the command that is configured under voice class takes precedence. Even when **no h225 display-ie ccm-compatible system** command is configured under voice service voip, the gateway will not send the H225 Notify message received, and the calling name does not display on the IP Phone.

  Use the **no** version to disable sending H225 Notify message on a particular VoIP dial-peer. The **no** form of the command is shown under voice class in the **show running-configuration**.

Examples

The following example shows a gateway being configured to send H.225 Notify message that displays the calling name on an IP Phone.

```
voice class h323 1
h225 display-ie ccm-compatible system
```

Related Commands

Command	Description
show running-configuration	Displays the contents of the currently running configuration file.

h225 h245-address

To control sending an H.245 address to a remote site use the **h225 h245-address** command in H.323 voice service configuration mode or to a H.323 voice class in global configuration mode. To disable the delay in sending H.245 address in H.225 messages, use the **no** form of this command.

h225 h245-address {**facility** | **listen-on-setup** | **on-alert** | **on-progress**}

no h225 h245-address

Syntax Description

facility	Provides IP-to-IP H.245 address reporting via the H.225 Facility msg.
listen-on-setup	IP-to-IP invokes H.245 listener if the H.245 address received in setup.
on-alert	Specifies the H.225 address on alerting control.
on-progress	Specifies the H.225 address progress control.

Defaults

The H.245 address is sent in H.225 Callproceeding message.

Command Modes

Voice service H.323 configuration (conf-serv-h323)
H.323 voice class (config-class)

Command History

Release	Modification
12.4(15)T7	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **h225 h245-address on-alert** command controls sending the local H.245 address to the remote side. Configuring the **h225 h245-address on-alert** command forces the Cisco IOS gateway to send the H.245 address in the H.225 alerting message instead of in the H.225 callproceeding message.

To configure the **h225 h245-address on-alert** command for a voice class. First create an H.323 voice class that is independent of a dial peer with the **voice class h323** command in global configuration mode and configure the **allow-connections** command.

Note The **voice-class h323** command in dial peer configuration mode includes a hyphen and in global configuration mode does not include a hyphen.

Examples

The following example globally delays the sending the H.245 transport address until call alerting happens:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address on-alert
```

The following example shows listen-on-setup capability configured mode after creating a voice class in global configuration mode and configuring the required **allow-connections** command:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# allow-connections H323 to h323
Router(conf-voi-serv)# exit

Router(config)# voice class h323 5
Router(config-class)# h225 h245-address listen-on-setup
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters Voice service H.323 configuration mode.
voice class h323	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers.
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service	Enters voice-service configuration mode.

h225 h245-address on-connect (H.323 voice-class)

To enable for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made, use the **h225 h245-address on-connect** command in H.323 voice-class configuration mode. To disable the delay of H.225 messages, use the **no** form of this command.

h225 h245-address on-connect

no h225 h245-address on-connect

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages that contain H.245 addresses are delayed until calls are connected.

Command Modes

H.323 voice-class configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The functionality specified by this command allows Cisco CallManager Express 3.1 (Cisco CME 3.1) or later systems to interwork with Cisco CallManager in the same network. This command should always be enabled.

When simple A-to-B calls are made from a Cisco CallManager phone to a Cisco CME IP phone, the Cisco CallManager must play in-band ringback tone locally to the originating phone. The Cisco CallManager stops the tone generation if it receives the call's H.245 address before the call is answered. The **h225 h245-address on-connect** command ensures that the H.245 address is not sent before the call is answered (connected). This command is enabled by default unless the **no** form of this command has been used. In addition, the **telephony-service ccm-compatible** command must also be enabled to detect calls from Cisco CallManager, which is the default.

This command can also be used in an H.323 voice-service definition to globally enable or disable this behavior.

Examples

The following example creates a voice class with the tag of 4, which delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made. Voice class 4 is then applied to dial peer 36.

```
Router(config)# voice class h323 4
Router(config-voice-class)# h225 h245-address on-connect

Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
h225 h245-address on-connect (H.323 voice-service)	Globally delays the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
telephony-service ccm-compatible (H.323 voice-class)	For an individual dial peer, enables the detection of a Cisco CallManager system in the network.
telephony-service ccm-compatible (H.323 voice-service)	Globally enables the detection of a Cisco CallManager system in the network.
voice class	Enters voice-class configuration mode.

h225 h245-address on-connect (H.323 voice-service)

To globally delay the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made, use the **h225 h245-address on-connect** command in H.323 voice-service configuration mode. To globally disable the delay, use the **no** form of this command.

h225 h245-address on-connect

no h225 h245-address on-connect

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages that contain H.245 addresses are delayed until calls are connected.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The functionality specified by this command allows Cisco CallManager Express 3.1 (Cisco CME 3.1) or later systems to interwork with Cisco CallManager in the same network. This command should always be enabled.

When simple A-to-B calls are made from a Cisco CallManager phone to a Cisco CME IP phone, the Cisco CallManager must play in-band ringback tone locally to the originating phone. The Cisco CallManager stops the tone generation if it receives the call's H.245 address before the call is answered. The **h225 h245-address on-connect** command ensures that the H.245 address is not sent before the call is answered (connected). This behavior is the default when a Cisco CME system detects an incoming call from a Cisco CallManager unless the **no** form of this command has been used. In addition, the **telephony-service ccm-compatible** command must also be enabled to detect calls from Cisco CallManager, which is the default.

This command can also be used in an H.323 voice-class definition to enable or disable this behavior for individual dial peers.

Examples

The following example globally delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made.

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address on-connect
```

Related Commands

Command	Description
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters H.323 voice-service configuration mode.
telephony-service ccm-compatible (H.323 voice-service)	Globally enables detection of Cisco CallManager in a network for all dial peers.
telephony-service ccm-compatible (voice-class)	Enables Cisco CallManager detection in a network by individual dial peers.
voice service	Enters voice-service configuration mode.

h225 h245-address setup

To allow a gateway to connect to an H.245 address received simultaneously with the H.225 setup message use the **h225 h245-address setup** command in voice service configuration mode or a H.323 voice class in global configuration mode. To return to the default behavior, use the **no** form of this command.

h225 h245-address setup

no h225 h245-address setup

Syntax Description

setup	Connects the gateway to the H.245 address simultaneously with an incoming H.225 setup message.

Defaults

This command is disabled by default. The gateway does not connect to the H.245 address received along with the H.225 setup message.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
H.323 Voice class (config-class)

Command History

Release	Modification
12.4(15)T3	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configuring the **h225 h245-address setup** command allows the gateways to receive both the H.225 setup message simultaneously with the H.245 address message.

To configure the **h225 h245-address setup** command for a voice class. First create an H.323 voice class that is independent of a dial peer with the **voice class h323** command in global configuration mode and configure the **allow-connections** command.

Note The **voice-class h323** command in dial peer configuration mode includes a hyphen and in global configuration mode does not include a hyphen.

Examples

The following example shows the gateway globally configured to connect to the H.245 address received along with the H.225 setup message:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address setup
```

The following example shows the gateway configured in a voice-class to connect to the H.245 address received along with H.225 setup message:

```
Router(config)# voice class h323 12
Router(config-class)# h225 h245-address setup
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters Voice service H.323 configuration mode.
voice class h323	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers.
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service	Enters voice-service configuration mode.

h225 id-passthru

To enable video call connections to pass through between endpoints regardless of software version, use the **h225 id-passthru** command in H.323 voice-service configuration mode. To return to the default, use the **no** form of this command.

h225 id-passthru

no h225 id-passthru

Syntax Description

This command has no arguments or keywords.

Command Default

Video calls are completed on endpoints using the same software version.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Video calls complete when the endpoints are operating the same version of software. Use this command to allow connections between video endpoints that are using different software versions.

Examples

The following example allows video calls to connect when the polycom endpoints are using different software versions:

```
Router(config-serv-h323)# h225 id-passthru
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h225 plus-digit passthru

To prefix and pass the plus digit (+) into a phone number on an H.323 trunk, use the **h225 plus-digit passthru** command in H.323 voice service configuration mode. To stop passing of the plus digit into a phone number, use the **no** form of this command.

For releases prior to 15.1(3)T

h225 plus-digit-passthru-calling

no h225 plus-digit-passthru-calling

h225 plus-digit-passthru-called

no h225 plus-digit-passthru-called

For 15.1(3)T and later releases

h225 plus-digit passthru {**destination** | **source**}

no h225 plus-digit passthru {**destination** | **source**}

Syntax Description

destination	Prefixes and passes the plus digit (+) into a destination (called) number on an H.323 trunk.
source	Prefixes and passes the plus digit (+) into a source (calling) number on an H.323 trunk.

Command Default

The plus digit is not prefixed and passed into a called or a calling number on an H.323 trunk.

Command Modes

H.323 voice service configuration (conf-serv-h323)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)T	This command was modified. The **destination** and **source** keywords replaced **plus-digit-passthru-calling** and **plus-digit-passthru-called** for Cisco IOS Releaase 15.1(3)T and later releases.

Usage Guidelines

When a “+” is prefixed before the dialed digits, the carrier recognizes the call as an International call without the country specific international operator dial string. The leading "+" digit in a dial-peer match pattern is used to match a phone number with a leading "+" E.164 digit. It is not used as a regular expression symbol but is a valid E.164 digit that should be preserved across the VoIP network.

Examples

The following example shows how to add the plus digit for the calling number using the **h225 plus-digit passthru source** command:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 plus-digit passthru source
```

The following example shows how to add the plus digit for the called number using the **h225 plus-digit passthru destination** command:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 plus-digit passthru destination
```

h225 signal overlap

To activate overlap signaling to the destination gateway, use the **h225 signal overlap** command in H.225 voice-service configuration mode. To stop sending overlap signaling messages, use the **no** form of this command.

h225 signal overlap

no h225 signal overlap

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 signaling overlap is disabled.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.2(15)T11	This command was introduced.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The terminating gateway is responsible for collecting all the called number digits. This is implemented by the dial peers matching destination patterns. When H.225 signal overlap is configured on the originating gateway, it sends the SETUP to the terminating gateway once a dial-peer match is found. The originating gateway sends all further digits received from user to the terminating gateway using INFO messages until it receives a sending complete from the user. The terminating gateway receives the digits in SETUP and subsequent INFO messages and does a dial-peer match. If a match is found, it sends a SETUP with the collected digits to the PSTN. All subsequent digits are sent to the PSTN using INFO messages at which time the call is complete.

Examples

The following example enables overlap signalling on the H.225 gateway:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 signal overlap
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 start-h245

To hold the H.245 connection procedures until after the H.225 connections are made, use the **h225 start-h245** command in H.323 voice-class configuration mode. To disable the connection sequence, use the **no** form of this command.

h225 start-h245 on-connect

no h225 start-h245 on-connect

Syntax Description

on-connect	Starts the H.245 procedure upon call connection.

Command Default

By default, h225 start-h245 on-connect is disabled. In case of IP-to-IP gateway (IPIPGW), the outbound gateway echoes the same h245 address and port number sent by the remote endpoint.

Command Modes

H.323 voice-class configuration (config-voice-class)
H.323 voice-service (conf-serv-h323)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **h225 start-245 on-connect** command ensures that the H.245 address is not sent before the call is answered (connected).

Configure this command in H.323 voice-service configuration mode to globally enable or disable the connection behavior.

Examples

The following example shows a voice class with the tag of 4 being created, which delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made.

```
Router(conf-serv-h323)#h225 start-h245 on-connect
```

Related Commands

Command	Description
h225 h245-address on-connect (H.323 voice-service)	Globally delays the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
telephony-service ccm-compatible (H.323 voice-class)	Detects a Cisco CallManager system in the network for an individual dial peer.
telephony-service ccm-compatible (H.323 voice-service)	Detects a Cisco CallManager system in the network globally.
voice class	Enters voice-class configuration mode.

h225 timeout call-proceeding

To set the H.225 call-proceeding (T310) disconnect timer, use the **h225 timeout call-proceeding** command in either voice-service or dial peer configuration mode. To revert to the default, use the **no** form of this command.

h225 timeout call-proceeding *duration*

no h225 timeout call-proceeding

Syntax Description

duration	Call-proceeding timeout, in seconds. Range: 1 to 300. Default: 60.

Command Default

60 seconds

Command Modes

For all dial peers: Voice-service configuration
For a single dial peer: Dial peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to set a maximum duration for the time between call setup and call connect.

You can use this command in either of two configuration modes:

- For all peers: Use voice-service configuration mode by entering the **voice service voip** command
- For just a single dial peer: Use dial peer configuration mode for the desired dial peer by entering the **voice class h323** command.

Examples

The following example sets the disconnect timer for all dial peers:

```
Router(config)# voice service voip
Router(config-voi-serv)# h225 timeout call-processing 5
```

The following example sets the disconnect timer for a single dial peer:

```
Router(config)# voice class h323 1
Router(config-class)# h225 timeout call-processing 5
```

Related Commands

Command	Description
h225 timeout setup	Sets a timer for the response of the outgoing SETUP message.
h225 timeout tcp call-idle	Sets a timer for an idle call connection.

Command	Description
h225 timeout tcp establish	Sets an H.225 TCP timer for VoIP dial peers.
scenario-cause	Configures new Q.850 call-disconnect cause codes for use if an H.323 call fails.

h225 timeout keepalive

To disconnect H.323 calls when a TCP keepalive timeout occurs, use the **h225 timeout keepalive** command in H.323 voice-service configuration mode. To enable H.323 calls to remain active and ignore the TCP keepalive timeout, use the no form of this command.

h225 timeout keepalive

no h225 timeout keepalive

Syntax Description

This command has no arguments or keywords.

Command Default

TCP keepalives are enabled.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.2(15)T12	This command was introduced.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3(4)T5	This command was integrated into Cisco IOS Release 12.3(4)T5.

Usage Guidelines

When using the default configuration of the **h225 timeout keepalive** command, if a TCP timeout occurs on the H.225 channel, all active calls are disconnected and corresponding H.225 TCP sockets are closed.

When the **no h225 timeout keepalive** command is configured and a timeout occurs, the H.225 TCP socket is closed for all calls; Active TDM-IP calls will be preserved, but IP to IP calls are disconnected. In both cases the H.225 TCP socket is closed.

Note This command is visible in the running configuration only when the user configures the **no** form of the command.

Examples

The following example enables TCP keepalives on H.225 VoIP call control sessions:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout keepalive
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 timeout setup

To configure the timeout value for the response of the outgoing SETUP message, use the **h225 timeout setup** command in voice class configuration mode. To remove the timeout value, use the **no** form of this command.

h225 timeout setup *seconds*

no h225 timeout setup

Syntax Description

seconds	Timeout value for the response of the outgoing SETUP message, in seconds. Default is 15.

Command Default 15 seconds

Command Modes Voice class configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example configures a timeout setup value of 10 seconds:

```
Router(config-class)# h225 timeout setup 10
```

Related Commands

Command	Description
h225 timeout tcp call-idle	Sets a timer for an idle call connection.
h225 timeout tcp establish	Configures the H.225 TCP timeout.

h225 timeout t302

To set the t302 timer when using overlap signaling, use the **h225 timeout t302** command in H.225 voice-service configuration mode. To return to the default overlap signaling setting, use the **no** form of this command

h225 timeout t302 *seconds*

no h225 timeout t302 *seconds*

Syntax Description

seconds	Number of seconds for timeouts. Range: 1 to 30

Command Default

The t302 timer is disabled.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Use this command to establish the maximum amount of time allowed to complete the dial-peer match when H.225 signal overlap is configured on the originating gateway.

Examples

The following example allows 15 seconds for the t302 timer to complete the dial-peer match before timing out:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout t302 15
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.
h225 signal overlap	Activates overlap signaling to the destination gateway.

h225 timeout t304

To set the t304 timer when using overlap signaling, use the **h225 timeout t304** command in H.323 voice-service configuration mode. To return to the default overlap signaling setting, use the **no** form of this command.

h225 timeout t304 *seconds*

no h225 timeout t304 *seconds*

Syntax Description

seconds	Length of timeout, in seconds. The range is from 1 to 30. The default is 10.

Command Default

The timer is enabled and set to 10 seconds.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **h225 timeout t304** command to configure the maximum interdigit delay on the originating gateway when H.225 overlap signaling is configured. Configure this command for the H.323 call leg on the originating gateway. If this timer expires, the call is disconnected with a cause code 28 (invalid number).

Examples

The following example allows 12 seconds for the t304 timer to complete the dial-peer match before timing out:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout t304 12
```

Related Commands

Command	Description
h225 timeout t302	Sets the t302 timer when using overlap signaling.
h225 signal overlap	Activates overlap signaling to the destination gateway.
h323	Enables H.323 voice-service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 timeout tcp call-idle (H.323 voice-service)

To set a timer for an idle call connection, use the **h225 timeout tcp call-idle** command in voice service h323 configuration mode. To reset to the default, use the **no** form of this command.

h225 timeout tcp call-idle {**value** *value* | **never**}

no h225 timeout tcp call-idle

Syntax Description

value *value*	Timeout value, in minutes. Range is 0 to 1440. The default is 10. If you specify 0, the timer is disabled and the TCP connection is closed immediately after all the calls are cleared.
never	The connection is maintained permanently or until the other endpoint closes it.

Command Default 10 minutes

Command Modes H.323 voice-service configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command specifies the time to maintain an established H.225 TCP connection when there are no calls on that connection. If the timer expires, the connection is closed. If the timer is running and any new call is made on that connection, the timer stops. When all the calls are cleared on that connection, the timer starts again.

Examples The following example sets the timer for an idle call connection to 10 minutes:

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout tcp call-idle value 10
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h225 timeout tcp establish

To set the H.225 TCP timeout value for Voice over IP (VoIP) dial peers, use the **h225 timeout tcp establish** command in voice class configuration mode. To reset to the default, use the **no** form of this command.

h225 timeout tcp establish *seconds*

no h225 timeout tcp establish

Syntax Description

seconds	Number of seconds for the timeout. Range is 0 to 30. The default is 15. If you specify 0, the H.225 TCP timer is disabled.

Command Default

15 seconds

Command Modes

Voice class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 1700, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco AS5300, Cisco uBR900, and Cisco uBR924.

Examples

The following example sets a timeout of 10 seconds, which is associated with the H.323 voice class labeled 1:

```
voice class h323 1
 h225 timeout tcp establish 10
```

Related Commands

Command	Description
voice class h323	Establishes an H.323 voice class.

h225 timeut ntf

To enable Cisco Unified Communications Manager to interpret the calling name coming in the Display IE of H.225 facility message, use the **h225 timeout ntf** command in voice service or voice class configuration mode. To return to the default configuration, use the **no** form of this command.

h225 timeout ntf *milliseconds*

no h225 timeout ntf *milliseconds*

Syntax Description

milliseconds	Amount of time in milliseconds. Valid range is 50 to 5000.

Command Default

Disabled. The Cisco Unified Communications Manager ignores the IE and does not display the calling name on the IP phone.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12. 4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configure this command on the gateway to control the Q931 setup message. This command is configured in voice service or voice class configuration mode.

When Cisco Unified Communications Manager (Cisco Unified CM) is interworking with Cisco Gateways, The Cisco Unified CM can interpret the calling name coming in Display IE of H.225 Setup and H.225 Notify messages, and display the calling name on the Cisco IP Phone. Calling names sent in Display IE of the H.225 Facility message are not interpreted by default.

When the **h225 timeout ntf** command is configured on the Cisco gateway, if a Q931 Setup message with name-to-follow comes, the gateway will not send the H.225 Setup message and buffers it until the ntf timer expires, or a Q931 Facility message is received from ISDN side.

Note In the event the facility is received before the timer expires, the gateway will stop the buffer timer, extract the relevent information and send it to terming endpoint.

When a Cisco gateway is connected to ISDN switches that send name-to-follow in Q931 Setup and the calling name in subsequent Q931 Facility message, configuring the **h225 timeout ntf** command is recommended.

Examples

The following example shows how to set the ntf buffering time to 60 milliseconds in the voice servides configuration mode:

```
voice service voip
 h323
  h225 timeout ntf 60
```

The following example sshows hotto se the ntf buffering time to 1000 milliseconds in the voice class configuration mode:

```
voice class h323 1
 h225 timeout ntf 1000
```

h245 address-check

To close the TCP connection of the endpoint with the numerically smaller H.245 address when two endpoints simultaneously initiate separate H.245 connections, use the **h245 address-check** command in H.323 voice-service configuration mode. To return to the default behavior, use the **no** form of this command.

h245 address-check

no h245 address-check

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway automatically closes its TCP connection when the remote side TCP connection attempts to overwrite the data on the existing gateway TCP connection.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
15.0(**1**)M2	This command was introduced.

Usage Guidelines

The **h245 address-check** command causes the gateway to use IP addresses to determine which endpoint to close when TCP connections are opened simultaneously. The gateway TCP connection is closed only if the IP address is smaller.

Examples

The following example shows how to close the TCP connection of the endpoint with the numerically smaller H.245 address when two endpoints simultaneously initiate separate H.245 connections

```
Router(conf-serv-h323)# h245 address-check
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h245 passthru

To allow H.245 calls to pass through to the Cisco Unified CallManager when the IP-to-IP gateway sends an incorrect intercluster trunk (ICT) version, use the **h245 passthru** command in voice service configuration mode. To disable this command use, the **no** form of this command.

h245 passthru {**all** | **tcsnonstd-passthru**}

no h245 passthru {**all** | **tcsnonstd-passthru**}

Syntax Description

all	Passes non-standard codec through the IP-to-IP gateway.
tcsnonstd-passthru	Passes terminal capabilities set (TCS) non-standard parameter pass through (CCM data only).

Command Default This command is disabled.

Command Modes Voice service configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines When resuming a call that was placed on hold fails on a Cisco Unified CallManager, generally the call fails on the second Cisco Unified CallManager because the IP-to-IP gateway (IPIPGW) sends an incorrect intercluster trunk (ICT) version for the first Cisco Unified CallManager to the second Cisco Unified CallManager, and because the IPIPGW drops the non-standard fields in the callproc, alert, and connect messages from the second Cisco Unified CallManager to the first Cisco Unified CallManager. To resolve this behavior configure the **h245 passthru** command

Note For IP-to-IP gateway functionality the **allow-connections h323 to h323** command must be configured.

Examples The following example show how you configure h.245 to pass through to the Cisco Unified CallManager, regardless of the intercluster trunk (ICT) version:

```
Router(conf-serv-h323)#h245 passthru tcsnonstd-passthru
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.

h245 timeout olc

To set the timeout value for the OpenLogicalChannel (OLC) message, use the **h245 timeout olc** command in H.323 voice-service configuration mode. To disable the timeout value for the OLC message, use the **no** form of this command.

h245 timeout olc *timeout value*

no h245 timeout olc *timeout value*

Syntax Description

timeout value	Length of timeout value, in seconds. Range: 1 to 30. Default: 4.

Command Default

Timeout value for the OLC message is enabled and set to 4 seconds.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

After the originating gateway sends an OLC message during the H.245 procedure, it waits for 4 seconds for the terminating gateway to respond with an OLC acknowledgment. This behavior is enabled by default, and the timeout value of the OLC message is set to 4 seconds.

However, sometimes when a slow link, such as a satellite link, is involved in sending messages, a delay can occur. In that case, 4 seconds are not enough to receive OLC messages, and the call fails even when the terminating gateway had responded with OLC acknowledgment. To avoid the random dropping of VoIP calls, use the **h245 timeout olc** command to change the length of time that the originating gateway waits for OLC acknowledgment from the terminating gateway.

Examples

The following example sets the timeout value for the OLC message to 20 seconds. It also shows that you can change the setting to 15 seconds:

```
h245 timeout olc 20
h245 timeout olc 15
```

The following example sets the timeout value back to the default setting of 4 seconds:

```
no h245 timeout olc 15
```

The output of the **show run** command does not show the default setting; however, it does include the command if the timeout value is modified:

```
voice service voip
 h323
  h245 timeout olc 20
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h323

To enable the H.323 voice service configuration commands, use the **h323** command in voice service configuration mode.

h323

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Voice service configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example enters H.323 voice service configuration mode:

```
Router(conf-voi-serv)# h323
```

Related Commands

Command	Description
call start	Forces the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls.
h225 timeout setup	Configures the timeout value for the response of the outgoing SETUP message.
h225 timeout tcp call-idle	Sets a timer for an idle call connection.
session transport	Configures the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers.

h323 asr

To enable application-specific routing (ASR) and specify the maximum bandwidth for a proxy, use the **h323 asr** command in interface configuration mode. To remove a bandwidth setting but keep ASR enabled, use **no** form of this command.

h323 asr [**bandwidth** *max-bandwidth*]

no h323 asr [**bandwidth** *max-bandwidth*]

Syntax Description

bandwidth *max-bandwidth*	(Optional) Maximum bandwidth, in mbps on the interface. Range is from 1 to 10000000. The default is the interface bandwidth. If you specify a value greater than the interface bandwidth, the bandwidth defaults to the interface bandwidth.

Command Default

ASR is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

This command is independent of the **h323 interface** command.

Note Specifying the **no h323 asr bandwidth** *max-bandwidth command* removes the bandwidth setting but leaves ASR enabled. You must enter the **no h323 asr** command to disable ASR.

Examples

The following example enables ASR and specifies a maximum bandwidth of 10,000 kbps:

```
h323 asr bandwidth 10000
```

h323 call start

To force the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls, use the **h323 call start** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

h323 call start {**fast** | **slow**}

no h323 call start

Syntax Description

fast	Gateway uses H.323 Version 2 (Fast Connect) procedures.
slow	Gateway uses H.323 Version 1 (Slow Connect) procedures.

Command Default

fast

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later releases, H.323 Voice over IP (VoIP) gateways by default use H.323 Version 2 (Fast Connect) for all calls including those initiating RSVP. Previously, gateways used only Slow Connect procedures for RSVP calls. To enable Cisco IOS Release 12.1(3)XI gateways to be backward compatible with earlier releases of Cisco IOS Release 12.1 T, the **h323 call start** command forces the originating gateway to initiate calls using Slow Connect.

This **h323 call start** command is configured as part of the global voice-service configuration for VoIP services. It does not take effect unless the **call start system** voice-class configuration command is configured in the VoIP dial peer.

Examples

The following example selects Slow Connect procedures for the gateway:

```
voice service voip
 h323 call start slow
```

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
call start	Selects whether the H.323 gateway uses Fast Connect or Slow Connect procedures for the specific VoIP dial peer.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h323 gatekeeper

To specify the gatekeeper associated with a proxy and to control how the gatekeeper is discovered, use the **h323 gatekeeper** command in interface configuration mode. To disassociate the gatekeeper, use the **no** form of this command.

h323 gatekeeper [**id** *gatekeeper-id]* {**ipaddr** *ipaddr* [*port*] | **multicast**}

no h323 gatekeeper [**id** *gatekeeper-id]* {**ipaddr** *ipaddr* [*port*] | **multicast**}

Syntax Description

id *gatekeeper-id*	(Optional) Gatekeeper name. Typically, this is a Domain Name Server (DNS) name, but it can also be a raw IP address in dotted form. If this parameter is specified, gatekeepers that have either the default or explicit flags set for the subnet of the proxy respond. If this parameter is not specified, only those gatekeepers with the default subnet flag respond.
ipaddr *ipaddr* [*port*]	The gatekeeper discovery message is unicast to this address and, optionally, the port specified.
multicast	The gatekeeper discovery message is multicast to the well-known RAS multicast address and port.

Command Default

No gatekeeper is configured for the proxy

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.

Usage Guidelines

You must enter the **h323 interface** and **h323 h323-id** commands before using this command. The **h323 gatekeeper** command must be specified on your Cisco IOS platform or the proxy does not go online. The proxy uses the interface address as its RAS signaling address.

Examples

The following example sets up a unicast discovery to a gatekeeper whose name is unknown:

```
h323 gatekeeper ipaddr 192.168.5.2
```

The following example sets up a multicast discovery for a gatekeeper of a particular name:

```
h323 gatekeeper id gk.zone5.com multicast
```

Related Commands

Command	Description
h323 h323-id	Registers an H.323 proxy alias with a gatekeeper.
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 h323-id

To register an H.323 proxy alias with a gatekeeper, use the **h323 h323-id** command in interface configuration mode. To remove an H.323 proxy alias, use the **no** form of this command.

h323 h323-id *h323-id*

no h323 h323-id *h323-id*

Syntax Description

h323-id	Name of the proxy. It is recommended that this name be a fully qualified e-mail ID, with the domain name being the same as that of its gatekeeper.

Command Default No H.323 proxy alias is registered

Command Modes Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines Each entry registers a specified H.323 ID proxy alias to a gatekeeper. Typically, these aliases are either simple text strings or legitimate e-mail IDs.

Note You must enter the **h323 interface** command before using this command. The **h323 h323-id** command must be entered on the same interface as the **h323 gatekeeper** command. The proxy does not go online without the **h323 interface** command.

Examples The following example registers an H.323 proxy alias called proxy1@zone5.com with a gatekeeper:

```
h323 h323-id proxy1@zone5.com
```

Related Commands

Command	Description
h323 gatekeeper	Specifies the gatekeeper associated with a proxy and controls how the gatekeeper is discovered.
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 interface

To select an interface whose IP address is used by the proxy to register with the gatekeeper, use the **h323 interface** command in interface configuration mode. To reset to the default port, use the **no** version of the command and then the **h323 interface** command.

h323 interface [*port-number*]

no h323 interface [*port-number*]

Syntax Description

port-number	(Optional) Port number that the proxy listens on for incoming call-setup requests. Range is from 1 to 65356. The default port number for the proxy is 11,720 in -isx- or -jsx- Cisco IOS images. The default port number for the proxy is 1720 in -ix- Cisco IOS images, which do not contain the VoIP gateway.

Command Default

Default port number is image dependent as described in the Syntax Description.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.1(5)T	The ability to specify the proxy port number was added on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series and on the Cisco MC3810.

Usage Guidelines

At proxy startup, Cisco IOS software checks for the presence of the VoIP gateway subsystem. If the subsystem is found to be present, the proxy code opens and listens for call setup requests on the new port. The proxy then registers this port with the gatekeeper.

Examples

The following example configures Ethernet interface 0 for incoming call-setup requests:

```
interface ethernet0
 h323 interface
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.

Command	Description
h323 qos	Enables QoS on the proxy.
h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

h323 qos

To enable quality of service (QoS) on the proxy, use the **h323 qos** command in interface configuration mode. To disable QoS, use the **no** form of this command.

h323 qos {**ip-precedence** *value* | **rsvp** {**controlled-load** | **guaranteed-qos**}}

no h323 qos {**ip-precedence** *value* | **rsvp** {**controlled-load** | **guaranteed-qos**}}

Syntax Description

ip-precedence *value*	RTP streams set their IP precedence bits to the specified *value*.
rsvp controlled-load	Controlled load class of service.
rsvp guaranteed-qos	Guaranteed QoS class of service.

Command Default

No QoS is configured

Command Modes

Interface configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.

Usage Guidelines

You must execute the **h323 interface** command before using this command.

Both IP precedence and RSVP QoS can be configured by invoking this command twice with the two different QoS forms.

Examples

The following example enables QoS on the proxy:

```
interface Ethernet0
 ip address 172.21.127.38 255.255.255.192
 no ip redirects
 ip rsvp bandwidth 7000 7000
 ip route-cache same-interface
 fair-queue 64 256 1000
 h323 interface
 h323 qos rsvp controlled-load
 h323 h323-id px1@zone1.com
 h323 gatekeeper ipaddr 172.21.127.39
```

Related Commands

Command	Description
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 t120

To enable the T.120 capabilities on your router and to specify bypass or proxy mode, use the **h323 t120** command in interface configuration mode.

h323 t120 {bypass | proxy}

Syntax Description

bypass	Bypass mode. In this mode, the H.245 Open Logical Channel messages for T.120 data channels are passed unmodified through the proxy, and TCP connections for T.120 are established directly between the two endpoints of the H.323 call.
proxy	Proxy mode. In this mode, T.120 features function properly.

Command Default

Bypass mode

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200, and Cisco MC3810.

Usage Guidelines

The **no** form of this command has no function—the only possible commands are **h323 t120 bypass** and **h323 t120 proxy**.

Examples

The following example enables T.120 capabilities:

```
proxy h323
interface ethernet0
 h323 t120 proxy
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines which port the proxy listens on.

h323-annexg

To enable the border element (BE) on the gatekeeper and to enter BE configuration mode, use the **h323-annexg** command in gatekeeper configuration mode. To disable the BE, use the **no** form of this command.

h323-annexg *border-element-id* **cost** *cost* **priority** *priority*

no h323-annexg

Syntax Description

border-element-id	Identifier of the Annex G border element that you are provisioning. Possible values are any International Alphabet 5 (IA5) string, without spaces and up to 20 characters in length. The *border-element-id* argument associates the gatekeeper with the BE identifier that is configured on the BE.
cost *cost*	Cost associated with this Annex G border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range is from 1 to 99. Default is 50.
priority *priority*	Priority associated with this Annex G border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range is 1 to 99. The default is 50.

Command Default

Cost: 50
Priority: 50

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The Annex G border element must be configured using the **call-router** command before the gatekeeper can be associated with the Annex G border element. The **h323-annexg** command associates the gatekeeper with a previously configured Annex G border element and indicates that the gatekeeper should interact with the BE in address resolution.

Examples

The following example enables Annex G configuration for a BE named “be20”:

```
Router(config-gk)# h323-annexg be20 cost 10 priority 40
Router(config-gk-annexg)#
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
prefix	Restricts the prefixes for which the gatekeeper should query the Annex G BE.

h323-gateway voip bind srcaddr

To designate a source IP address for the voice gateway, use the **h323-gateway voip bind srcaddr** command in interface configuration mode. To remove the source IP address, use the **no** form of the command.

h323-gateway voip bind srcaddr *ip-address*

no h323-gateway voip bind srcaddr

Syntax Description

ip-address	Source IP address, in dotted-decimal notation.

Command Default

No default behaviors or values

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 1700, Cisco 2500, Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco S5300, and Cisco uBR924.

Usage Guidelines

You do not have to issue this command on the interface that you defined as the voice gateway interface (although it may be more convenient to do so). Use this command the interface that contains the IP address to which you want to bind.

Examples

The following example assigns a source IP address of 10.1.1.1:

```
h323-gateway voip bind srcaddr 10.1.1.1
```

h323-gateway voip h323-id

To configure the H.323 name of the gateway that identifies this gateway to its associated gatekeeper, use the **h323-gateway voip h323-id** command in interface configuration mode. To disable this defined gateway name, use the **no** form of this command.

h323-gateway voip h323-id *interface-id*

no h323-gateway voip h323-id *interface-id*

Syntax Description

interface-id	H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway with the gatekeeper domain name appended to the end and in name@domain-name.

Command Default No gateway identification is defined

Command Modes Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the gateway ID is GW13@cisco.com.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip id

To define the name and location of the gatekeeper for a specific gateway, use the **h323-gateway voip id** command in interface configuration mode. To disable this gatekeeper identification, use the **no** form of this command.

h323-gateway voip id *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**} [**priority** *number*]

no h323-gateway voip id *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**} [**priority** *number*]

Syntax Description

gatekeeper-id	H.323 identification of the gatekeeper. This value must exactly match the gatekeeper ID in the gatekeeper configuration. The recommended format is *name.doman-name*.
ipaddr	The gateway uses an IP address to locate the gatekeeper.
ip-address	IP address used to identify the gatekeeper.
port-number	(Optional) Port number used.
multicast	Indicates that the gateway uses multicast to locate the gatekeeper.
priority *number*	(Optional) Priority of this gatekeeper. Range is 1 to 127, 1 has the highest priority. The default is 127.

Command Default

No gatekeeper identification is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.0(7)T	The **priority** *number* keyword and argument were added.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command tells the H.323 gateway associated with this interface which H.323 gatekeeper to talk to and where to locate it. The gatekeeper ID configured here must exactly match the gatekeeper ID in the gatekeeper configuration.

You can configure one or two alternate gatekeepers.

The IP address of the gatekeeper does not have to be explicit; you can also use the multicast option. Multicasting saves bandwidth by forcing the network to replicate packets only when necessary. The multicast option, shown below, notifies every gatekeeper in the LAN using a universal address, 224.0.1.41.

```
h323-gateway voip id GK1 multicast
h323-gateway voip id GK2 ipaddr 172.18.193.65 1719
```

Examples

The following example configures Ethernet interface 0.0 as the gateway interface and defines a specific gatekeeper for it. In this example, the gatekeeper ID is GK15.cisco.com, and its IP address is 172.16.53.15 (using port 1719).

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip interface

To configure an interface as an H.323 gateway interface, use the **h323-gateway voip interface** command in interface configuration mode. To disable H.323 gateway functionality for an interface, use the **no** form of this command.

h323-gateway voip interface

no h323-gateway voip interface

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the **h323-gateway voip interface** command configures this interface as an H.323 interface.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip tech-prefix

To define the technology prefix that the gateway registers with the gatekeeper, use the **h323-gateway voip tech-prefix** command in interface configuration mode. To disable this defined technology prefix, use the **no** form of this command.

h323-gateway voip tech-prefix *prefix*

no h323-gateway voip tech-prefix *prefix*

Syntax Description

prefix	Numbers used as the technology prefixes. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound sign (#) is frequently used as the last digit in a technology prefix. Valid characters are 0 to 9, the pound sign (#), and the asterisk (*).

Command Default Disabled

Command Modes Interface configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command defines a technology prefix that the gateway then registers with the gatekeeper. Technology prefixes can be used as a discriminator so that the gateway can tell the gatekeeper that a certain technology is associated with a particular call (for example, 15# could mean a fax transmission), or it can be used like an area code for more generic routing. No standard currently defines what the numbers in a technology prefix mean. By convention, technology prefixes are designated by a pound sign (#) as the last character.

Note Cisco gatekeepers use the asterisk (*) as a reserved character. If you are using Cisco gatekeepers, do not use the asterisk as part of the technology prefix.

Examples

The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the technology prefix is defined as 13#.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323-gateway voip interface	Configures an interface as an H.323 interface.

h323zone-id (voice source group)

To specify the zone identification for an incoming H.323 call, use the **h323zone-id** command in voice source-group configuration mode. To delete the zone ID, use the **no** form of this command.

h323zone-id *name*

no h323zone-id *name*

Syntax Description

name	Zone ID name. Maximum size is 127 alphanumeric characters.

Command Default No default behavior or values

Command Modes Voice source-group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to specify the zone to use for incoming H.323 calls in the voice source-group definition. The zone ID name matches the source zone ID of an incoming H.323 call.

Note The SIP protocol does not support zone ID functionality.

Examples The following example associates zone ID "5400-gw1" with incoming calls for source IP group "northcal":

```
Router(config)# voice source-group northcal
Router(cfg-source-grp)# h323zone-id 5400-gw1
```

Related Commands

Command	Description
voice source-group	Defines a source group for voice calls.

h450 h450-3 timeout

To specify timeout values for call forwarding using the ITU-T H.450.3 standard, use the **h450 h450-3 timeout** command in H.323 voice service configuration mode. To return to the default, use the **no** form of this command.

h450 h450-3 timeout T1 *milliseconds*

no h450 h450-3 timeout T1

Syntax Description

T1	Timeout value to wait for a rerouting response.
milliseconds	Number of milliseconds. Range is from 500 to 60000. Default is 5000.

Command Default

T1 timer is 5000 milliseconds.

Command Modes

H323 voice service configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use this command with Cisco IOS Telephony Service (ITS) V2.1 or a later version.

This command is primarily used when the default setting for this timer does not match your network delay parameters. Refer to the ITU-T H.450.3 specification for more information on these timers.

Examples

The following example defines a T1 timeout of 3000 milliseconds:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h450 h450-3 timeout T1 3000
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode.

handle-replaces

To configure a Cisco IOS device to handle Session Initiation Protocol (SIP) INVITE with Replaces header messages at the SIP protocol level, use the **handle-replaces** command in SIP UA configuration mode. To return to the default handling of SIP INVITE with Replaces header messages where messages are handled at the application layer, use the **no** form of this command.

handle-replaces

no handle-replaces

Syntax Description

This command has no arguments or keywords.

Command Default

Handling of SIP INVITE with Replaces header messages takes place at the application layer.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

On Cisco IOS devices running software earlier than Cisco IOS Release 12.4(22)T, SIP INVITE with Replaces header messages (such as those associated with Call Replacement during a Consult Call transfer scenario) are handled at the SIP protocol level. Beginning with Cisco IOS Release 12.4(22)T, the default behavior is for Cisco IOS devices to handle SIP INVITE with Replaces header messages at the application layer. To configure your Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level, use the **handle-replaces** command in SIP UA configuration mode.

Examples

The following example shows how to configure fallback to legacy handling of SIP INVITE messages:

```
Router(config)# sip-ua
Router(config-sip-ua)# handle-replaces
```

Related Commands

Command	Description
supplementary-service sip	Enables SIP supplementary service capabilities for call forwarding and call transfers across a SIP network.

hangup-last-active-call

To define a Feature Access Code (FAC) to access the Hangup Last Active Call feature in feature mode on analog phones connected to FXS ports, use the **hangup-last-active-call** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

hangup-last-active-call *keypad-character*

no hangup-last-active-call

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0—9, *, #). Default is #1.

Command Default

The default value is #1.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for the Hangup Last Active Call feature from the default (#1) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Note For analog phones connected to FXS ports in Cisco Unified Communications Manager Express (CME), the **keep-conference drop-last** command must be enabled on the Cisco router.

Examples

The following example shows how to change the value of the feature code for the Hangup Last Active Call feature from the default (#1). With this configuration, a phone user must press hook flash during a three-party conference to get the feature tone and then dial 11 to drop the last active call party. The conference becomes a basic call.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# hangup-last-active-call 11
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

header-passing

To enable the passing of headers to and from Session Initiation Protocol (SIP) INVITE, SUBSCRIBE, and NOTIFY messages, use the **header-passing** command in voice service voip sip configuration mode. To disable header passing, use the **no** form of this command.

header-passing

no header-passing

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

voice service voip sip configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- This command applies to all SIP VoIP dial peers configured on a gateway. It enables header passing for SIP INVITE, SUBSCRIBE and NOTIFY messages; disabling header passing affects only incoming INVITE messages.
- There is no command to enable header passing on a per-call or per-application basis.
- Enabling header passing results in a slight increase in memory and CPU utilization.

Examples

The following example shows header-passing enabled:

```
Router(conf-serv-sip)# header-passing
```

Related Commands

Command	Description
debug voip ccapi protoheaders	Displays messages related to protocol headers.
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
show subscription sip	Displays active SIP subscriptions.
subscription maximum originate	Specifies the maximum number of outstanding subscriptions that are originated by the gateway.

history-info

To enable Session Initiation Protocol (SIP) history-info header support on Cisco IOS gateway at a global level, use the **history-info** command in voice service voip sip configuration mode. To disable SIP history-info header support, use the **no** form of this command.

history-info

no history-info

Syntax Description

This command has no keywords or arguments.

Command Default

History-info header support is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use this command to enable history-info header support at a global level. The history-info header (as defined in RFC 4244) records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.

Note The Cisco IOS SIP gateway cannot use the information in the history-info header to make routing decisions.

Examples

The following example enables SIP history-info header support:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# history-info
```

Related Commands

Command	Description
voice-class sip history-info	Enables SIP history-info header support at the dial-peer level.

history session event-log save-exception-only

To save in history only the event logs for application sessions that have at least one error, use the **history session event-log save-exception-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session event-log save-exception-only

no history session event-log save-exception-only

Syntax Description

This command has no arguments or keywords.

Command Default

All event logs for sessions are saved to history.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session event-log save-exception-only** command.

Usage Guidelines

Application event logs move from active to history after an instance terminates. If you use this command, the voice gateway saves event logs only for instances that had one or more errors. Event logs for normal instances that do not contain any errors are not saved to history.

Note This command does not affect records saved to an FTP server by using the **dump event-log** command.

Examples

The following example saves an event log in history only if the instance had an error:

```
application
 monitor
 history session event-log save-exception-only
```

Related Commands

Command	Description
call application history session event-log save-exception-only	Saves in history only the event logs for application sessions that have at least one error.
history session max-records	Sets the maximum number of application instance records saved in history.
history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.

history session max-records

To set the maximum number of application instance records saved in history, use the **history session max-records** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session max-records *number*

no history session max-records

Syntax Description

number	Maximum number of records to save in history. Range is 0 to 2000. Default is 360.

Command Default

360

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session max-records** command.

Usage Guidelines

This command affects the number of records that display when you use the **show call application history session-level** command.

Examples

The following example sets the maximum record limit to 500:

```
application
 monitor
 history session max-records 500
```

Related Commands

Command	Description
call application history session max-records	Sets the maximum number of application instance records saved in history.
history session event-log save-exception-only	Saves in history only the event logs for application sessions that have at least one error.
history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.

history session retain-timer

To set the maximum number of minutes for which application instance records are saved in history, use the **history session retain-timer** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session retain-timer *minutes*

no history session retain-timer

Syntax Description

minutes	Maximum time, in minutes, for which history records are saved. Range is 0 to 4294,967,295. Default is 15.

Command Default 15

Command Modes Application configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session retain-timer** command.

Usage Guidelines This command affects the number of records that display when you use the **show call application history session-level** command.

To enable event logging for voice applications, use the **event-log** command.

Examples The following example sets the maximum time to save history records to 1 hour:

```
application
 monitor
 history session retain-timer 60
```

Related Commands

Command	Description
call application history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
event-log	Enables event logging for voice application instances.
history session event-log save-exception-only	Saves in history only the event logs for application instances that have at least one error.

Command	Description
history session max-records	Sets the maximum number of application instance records saved in history.
show call application session-level	Displays event logs and statistics for voice application instances.

hold-resume

To enable the Hold/Resume STC application supplementary-service feature on an FXS port, use the **hold-resume** command in supplementary-service voice-port configuration mode. To disable, use the **no** form of this command.

hold-resume

no hold-resume

Syntax Description

This command has no arguments or keywords.

Command Default

Feature is disabled.

Command Modes

Supplementary-service voice-port configuration (config-stcapp-suppl-serv-port)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables the Hold/Resume STC application supplementary-service feature on analog endpoints that are connected to FXS ports on a Cisco IOS voice gateway, such as a Cisco integrated services router (ISR) or Cisco VG224 Analog Phone Gateway.

Examples

The following example shows how to enable Hold/Resume on port 2/0 on a Cisco VG 224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STC application supplementary-service features on an FXS port.

hopcount

To specify the maximum number of border element (BE) hops through which an address resolution request can be forwarded, use the **hopcount** command in Annex G configuration mode. To restore the default, use the **no** form of this command.

hopcount *hopcount-value*

no hopcount

Syntax Description

hopcount-value	Maximum number of BE hops through which an address resolution request can be forwarded. Range is from 1 to 255. The default is 7.

Command Default 7 hops

Command Modes Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example sets address-resolution forwarding to a maximum of 10 hops:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# hopcount 10
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
show call-router status	Displays the Annex G BE status.

host (SIP URI)

To match a call based on the host field, a valid domain name, IPv4 address, IPv6 address, or the complete domain name in a Session Initiation Protocol (SIP) uniform resource identifier (URI), use the **host** command in voice URI class configuration mode. To remove the host match, use the **no** form of this command.

host {**ipv4:***ipv4-address* | **ipv6:***ipv6-address* | **dns:***dns-name* | *hostname-pattern*}

no host

Syntax Description

ipv4:*ipv4-address*	Specifies a valid IPv4 address.
ipv6:*ipv6-address*	Specifies a valid IPv6 address.
dns:*dns-name*	Specifies a valid domain name. The maximum length of a valid domain name is 64 characters.
hostname-pattern	Cisco IOS regular expression pattern to match the host field in a SIP URI. The maximum length of a hostname pattern is 32 characters.

Command Default

The calls are not matched on the host field, IPv4 address, IPv6 address, valid domain name, or complete domain name in the SIP URI.

Command Modes

Voice URI class configuration (config-voice-uri-class)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The **ipv4:***ipv4-address*, **ipv6:***ipv6-address*, and **dns:***dns-name* arguments were included.

Usage Guidelines

You can use this command only in a voice class for SIP URIs.

You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

You can configure ten instances of the **host** command by specifying IPv4 addresses, IPv6 addresses, or domain name service (DNS) names for each instance. You can configure the **host** command specifying the *hostname-pattern* argument only once.

Examples

The following example defines a voice class that matches on the host field in a SIP URI:

```
voice class uri r100 sip
  user-id abc123
  host server1
  host ipv4:10.0.0.0
  host ipv6:[2001:0DB8:0:1:FFFF:1234::5]
  host dns:example.sip.com
  phone context 408
```

Related Commands

Command	Description
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

host-registrar

To populate the sip-ua registrar domain name or IP address value in the host portion of the diversion header and to redirect the contact header of the 302 response, use the **host-registrar** command in SIP user-agent configuration mode. To remove the sip-ua registrar domain name or IP address from the host portion of the diversion and redirect contact headers, use the **no** form of this command.

host-registrar

no host-registrar

Syntax Description

This command has no arguments or keywords.

Command Default

This command's functionality is disabled. In the default condition, diversion headers are populated with the domain name or IP address of the gateway, and redirect contact headers are populated with the dial peer session target IP address or hostname.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

You must first configure the **sip-ua** command to place the router in SIP user-agent configuration mode before you can use the **host-registrar** command.

By default, the Session Initiation Protocol (SIP) gateway and Cisco Unified Communications Manager Express (Cisco Unified CME) populate the host portion of the diversion header with the domain name or IP address of the gateway that generates the request or response. The SIP gateway and Cisco Unified CME also populate the host portion of the redirect contact header with the session target IP address or hostname of the matching dial peer.

When the **host-registrar** command and the **registrar** command are both configured in SIP user-agent configuration mode, the SIP gateway or Cisco Unified CME populate the host portion of both the diversion and redirect contact headers with the domain name or IP address configured by the **registrar** command.

The **host-registrar** command should be configured along with the **registrar** command in SIP user-agent configuration mode. If the **host-registrar** command is configured without the **registrar** command, the host portion of the diversion header is populated with the domain name or IP address of the gateway and the host portion of the redirect contact header is populated with the session target IP address or hostname of the matching dial peer.

Examples

The following example shows how to configure the **host-registrar** and **registrar** commands in SIP user-agent configuration mode to specify a URL scheme with SIP security:

```
sup-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar dns:example.com scheme sips
 host-registrar
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164-numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
sip-ua	Enables SIP user-agent configuration commands and configures the user agent.

http client cache memory

To set the memory file and pool limits for the HTTP client cache, use the **http client cache memory** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client cache memory {**file** *file-size* | **pool** *pool-size*}

no http client cache memory {**file** | **pool**}

Syntax Description

file *file-size*	Maximum file size, in kilobytes, allowed for caching. Any file that is larger is not cached. Range is 1 to 10000. The default is 50.
pool *pool-size*	Maximum pool size, in kilobytes, allowed for caching. Range is 0 to 100000. The default is 10000. Setting the memory pool size to 0 disables HTTP caching.

Command Default

Memory file size: 50 KB
Memory pool size: 10 MB

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.3(5)	The default for the *file-size* argument was increased from 2 to 50 KB and the default of the *pool-size* argument was increased from 100 to 10000 KB.
12.3(7)T	The default changes in Cisco IOS Release 12.3(5) were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

A larger cache size may permit caching of frequently used files, decreasing the fetching time between the client and server and increasing performance. Allocation of memory to increase file size or pool size does not reduce the amount of memory available. Cache memory is used only when needed, and afterward returns to being memory shared with other resources.

The amount of memory required for an expected level of performance depends on a number of factors, including the type of voice gateway (for example, Cisco 2600 series or Cisco AS5400).

The recommended maximum file size is 10 MB; the recommended maximum pool size is 100 MB.

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

Note For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following example sets the HTTP client cache memory pool to 50,000 KB:

```
http client cache memory pool 50000
```

The following example sets the HTTP client cache memory file to 8000 KB:

```
http client cache memory file 8000
```

Related Commands

Command	Description
http client cache refresh	Configures the refresh time for the HTTP client cache.
http client connection idle timeout	Configures the HTTP client connection.
http client response timeout	Configures the HTTP client server response.
show http client cache	Displays current HTTP client cache information.

http client cache query

To enable caching of query data returned from the HTTP server, use the **http client cache query** command in global configuration mode. To disable caching of query data, use the **no** form of this command.

http client cache query

no http client cache query

Syntax Description This command has no arguments or keywords.

Command Default Query data is not cached.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines Use the **show http client cache** command to display cached query data. To protect caller privacy, values of the URL attributes are masked out with asterisks (*) in the **show http client cache** command output. If you use this command to enable caching of query data, use the **http client cache memory** command to increase the size of the HTTP client cache memory pool to accommodate the cached query data.

Examples The following example enables caching of query data returned from the HTTP server:

```
Router# http client cache query
```

Related Commands

Command	Description
http client cache memory	Sets the memory file and pool limits for the HTTP client cache.
show http client cache	Displays information about the entries contained in the HTTP client cache.

http client cache refresh

To set the time limit for how long a cached entry is considered current by the HTTP client, use the **http client cache refresh** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client *cache* refresh *seconds*

no http client cache refresh

Syntax Description

seconds	Lifetime of a cached HTTP entry, in seconds. Range is from 1 to 864000. The default is 86400 (24 hours).

Command Default 86,400 seconds (24 hours)

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines This command must be used to set the refresh time only if the HTTP server does not provide the necessary information in the HTTP header to calculate this value.

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

When a request is made to an expired cached entry (that is, an entry that is the same age as or older than the refresh time), the HTTP client sends the server a conditional request for an update.

An expired entry is not automatically updated unless a request from the user hits the same cached entry. Expired entries are not cleaned up until 70 percent or more of the cache pool memory is consumed; then all expired entries that lack a user reference are deleted from the cache table.

Note For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples The following example shows the HTTP client cache refresh to be 10 seconds:

```
http client cache refresh 10
```

Related Commands

Command	Description
http client cache memory	Configures the memory limits for the HTTP client cache.
http client connection idle timeout	Configures the HTTP client connection.
http client response timeout	Configures the HTTP client server response.
show http client cache	Displays current HTTP client cache information.

http client connection idle timeout

To set the number of seconds for which the HTTP client waits before terminating an idle connection, use the **http client connection idle timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client connection idle timeout *seconds*

no http client connection idle timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits before terminating an idle connection. Range is from 1 to 60. The default is 2.

Command Default 2 seconds

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines The setting of this command determines when the HTTP client is disconnected from the HTTP server, which is necessary when the server does not disconnect the client after a desirable length of time.

The default value is recommended and should normally not be changed.

In the **show http client connection** command output, this parameter is displayed as *connection idle timeout.*

The gateway might accept invalid characters such as “#” or “!” when you input the value for this command. The gateway ignores any invalid characters.

Examples The following example sets the timeout to 40 seconds:

```
http client connection idle timeout 40
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client connection persistent

To enable HTTP persistent connections so that multiple files can be loaded using the same connection, use the **http client connection persistent** command in global configuration mode. To disable HTTP persistent connections, use the **no** form of this command.

http client connection persistent

no http client connection persistent

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent connections are enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

The setting of this command determines whether the HTTP client requests a keepalive or closed connection from the server. The HTTP server is responsible for granting or denying the keepalive connection request from the client.

Enabling persistent connections is recommended.

In the **show http client connection** command output, activation of this command is displayed as *persistent connection.*

Examples

The following example shows the HTTP client connection persistent parameter to be enabled:

```
http client connection persistent
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client connection timeout

To set the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt, use the **http client connection timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client connection timeout *seconds*

no http client connection timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits for a server to establish a connection before abandoning its connection attempt. Range is from 1 to 60. The default is 5.

Command Default 5 seconds

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines The setting of this command determines when the HTTP client abandons its attempt to connect to the server, which is necessary when a connection to the server cannot be established after a desirable length of time.

The default value is recommended and should normally not be changed.

In the **show http client connection** command output, activation of this command is displayed as *initial socket connection timeout.*

The gateway might accept invalid characters such as “#” or “!” when you input the value for this command. The gateway ignores any invalid characters.

Examples The following example shows the HTTP client connection timeout parameter to be 20 seconds:

```
http client connection timeout 20
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client cookie

To enable the HTTP client to send and receive cookies, use the **http client cookie** command in global configuration mode. To disable cookie support, use the **no** form of this command.

http client cookie

no http client cookie

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines This command enables RFC 2109-compliant support with the following exceptions:

- Cookies cannot be cached.
- Maximum number of cookies that are stored for a call is 10. If this limit is reached, any subsequent cookies are discarded when they are received.
- Cookies are only maintained for the duration of the call; when a call terminates, all associated cookies are discarded.
- Secure method is not supported.

Examples The following example enables HTTP cookie support if it was previously disabled using the **no http client cookie** command:

```
Router(config)# http client cookie
```

Related Commands

Command	Description
debug http client cookie	Displays debugging traces related to HTTP cookies.
http client cache memory	Configures the memory limits for the HTTP client cache.
http client cache refresh	Configures the refresh time for the HTTP client cache.
show http client cookie	Displays cookies that are being stored by the HTTP client.

http client post-multipart

To configure the HTTP client to generate a filename string that is not enclosed in quotation marks, use the **http client post-multipart content-disposition filename no-quote** command in global configuration mode. To return to the default, use the **no** form of this command.

http client post-multipart content-disposition filename no-quote

no http client post-multipart content-disposition filename no-quote

Syntax Description

content-disposition filename no-quote	HTTP client generates a filename string that is not enclosed in quotation marks.

Command Default

Filename string is enclosed in quotation marks.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

In a multipart HTTP POST request, the HTTP client on the router generates the filename string enclosed in quotation marks (“”). Although the Multipurpose Internet Mail Extension (MIME) standard recommends that quotation marks be used, some HTTP servers conform to RFC 2068, which does not include quotation marks. Some older Hypertext Preprocessor (PHP) files require that the filename string be embedded in quotation marks. Use the **http client post-multipart** command to remove the quotation marks from the filename if you do not need them.

Examples

The following example configures the HTTP client to generate filenames that are not enclosed in quotation marks in a multipart POST request:

```
Router# http client post-multipart content-disposition filename no-quote
```

http client response timeout

To configure the number of seconds for which the HTTP client waits for a server response, use the **http client response timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client response timeout *seconds*

no http client response timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits for a response from the server after making a request. Range is from 1 to 300. The default is 10.

Command Default

10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command is used to adjust the time allowed for the HTTP client to wait for the server to respond to a request before declaring a timeout error. Under normal conditions, the default of 10 seconds is sufficient. If more or less server response time is desired, use this command. For example, if your server responds slowly to the HTTP client requests, you may want to set this timer to wait longer.

In the **show running-config** command output, the value is displayed only if it is set to other than the default.

The gateway might accept invalid characters such as “#” or “!” when you input the value for this command. The gateway ignores any invalid characters.

Examples

The following example shows the HTTP client response timeout to be 5 seconds:

```
http client response timeout 5
```

Related Commands

Command	Description
show http client cache	Displays the HTTP client cache.
show http client connection	Displays the HTTP client connection.

http client secure-ciphersuite

To set the secure encryption cipher suite for the HTTP client, use the **http client secure-ciphersuite** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client secure-ciphersuite {[**3des_cbc_sha**] [**des_cbc_sha**] [**null_md5**] [**rc4_128_md5**] [**rc4_128_sha**]}

no http client secure-ciphersuite

Syntax Description

3des_cbc_sha	Triple DES (Data Encryption Standard) encryption and the SHA (Secure Hash Algorithm) integrity method. The first portion of the keyword indicates the encryption; the last portion indicates the hash or integrity method.
des_cbc_sha	DES encryption and the SHA integrity method.
null_md5	NULL encryption and the MD5 (Message-Digest algorithm 5) integrity method.
rc4_128_md5	RC4 (or ARCFOUR) encryption and the MD5 integrity method.
rc4_128_sha	RC4 encryption and the SHA integrity method.

Command Default

All cipher suites.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use this command to configure one or more cipher suites, or sets of encryption and hash algorithms, on the HTTP client. You must include at least one of the keywords and can include more than one. Use the **show http client secure status** command to display the cipher suites configured.

Examples

The following example sets the HTTP client to use the 3des_cbc_sha and null_md5 cipher suites:

```
Router(config)# http client secure-ciphersuite 3des_cbc_sha null_md5
```

Related Commands

Command	Description
http client secure-trustpoint	Declares the trustpoint that the HTTP client should use for HTTPS sessions.
show http client secure status	Displays the trustpoint and cipher suites that are configured in the HTTP client.

http client secure-trustpoint

To declare the trustpoint that the HTTP client will use for HTTPS (HTTP over Secure Socket Layer (SSL)) sessions, use the **http client secure-trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

http client secure-trustpoint *name*

no http client secure-trustpoint *name*

Syntax Description

name	Creates a name for the secure certification authority (CA) trustpoint.

Command Default

The Public Key Infrastructure (PKI) trustpoint configured on the router, or the primary trustpoint if more than one trustpoint is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **show http client secure status** command to display the trustpoints and cipher suites configured for the client.

Examples

The following example sets the HTTP client's secure CA trustpoint to myca:

```
Router(config)# http client secure-trustpoint myca
```

Related Commands

Command	Description
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.
show http client secure status	Displays the trustpoint and cipher suites that are configured in the HTTP client.

hunt-scheme least-idle

To enable the least-idle search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme least-idle** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of the command.

hunt-scheme least-idle [**both** | **even** | **odd**]

no hunt-scheme

Syntax Description

both	(Optional) Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel with the shortest idle time. If no idle even-numbered channel is available, an odd-numbered channel with the longest idle time is sought.
odd	Searches for an idle odd-numbered channel with the shortest idle time. If no idle odd-numbered channel is available, an even-numbered channel with the longest idle time is sought.

Command Default

Hunt scheme: least-used
Channel number: **both**

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the least-idle hunt scheme in situations where you want to reuse the most recently selected channel.

The least-idle hunt scheme looks for the channel that has just become available. The software looks at all the channels in the trunk group, regardless of member precedence, and selects the channel that has most recently come into the available queue.

If no channels are available at the time of the call request, the software returns a cause code determined by the application configured on the inbound dial peer.

If the **even** quantifier is set, the even-numbered channel with the shortest idle time is selected. If the **odd** quantifier is set, the odd-numbered channel with the shortest idle time is selected. If **both** is set, the most recently available channel, regardless of channel number, is selected.

Examples

The following example searches for an even-numbered idle channel having the shortest idle time within a trunk group:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme least-idle even
```

Related Commands

Command	Description
hunt-scheme longest-idle	Enables the longest-idle hunt scheme.
trunk group	Initiates a trunk group profile.

hunt-scheme least-used

To enable the least used search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme least-used** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of the command.

hunt-scheme least-used [**both** | **even** | **odd** [**up** | **down**]]

no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channels are available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channels are available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used
Channel number: both
Direction: up

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The least-used search method selects an idle channel from a trunk group member that has the highest number of available channels at the time that the hunt request is initiated. The high number of unused channels indicates that the trunk group member has not been very active in comparison with other trunk group members.

After selecting the trunk group member, the software searches the channels by direction and then by channel number:

- If **even up** is set, the software searches the trunk group members in ascending order of preference to determine which member has the highest number of available even-numbered channels. If no available even-numbered channel is found, the software searches the members again in ascending order for the member that has the highest number of available odd-numbered channels.

- If **odd up** is set, the software searches the trunk group members in ascending order of preference to determine which member has the highest number of available odd-numbered channels. If no available odd-numbered channel is found, the software searches the members again in ascending order for the member that has the highest number of available even-numbered channels.
- If **even down** is set, the software searches in descending order of preference to determine which member has the highest number of available even-numbered channels. If no available even-numbered channel is found, the software searches the members again in descending order for the member that has the highest number of available odd-numbered channels.
- If **odd down** is set, the software searches in descending order of preference to determine which member has the highest number of available odd-numbered channels. If no available odd-numbered channel is found, the software searches the members again in descending order for the member that has the highest number of available even-numbered channels.

If no channel is available in any of the trunk group members, the software returns the standard "no service" message.

Examples

The following example searches in ascending order for an even-numbered idle channel in a trunk group member having the highest number of available channels:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme least-used even up
```

Related Commands

Command	Description
trunk group	Initiates a trunk group profile.

hunt-scheme longest-idle

To enable the longest-idle search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme longest-idle** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme longest-idle [**both** | **even** | **odd**]

no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel with the longest idle time. If no idle even-numbered channel is available, an odd-numbered channel with the shortest idle time is sought.
odd	Searches for an idle odd-numbered channel with the longest idle time. If no idle odd-numbered channel is available, an even-numbered channel with the shortest idle time is sought.

Command Default

Hunt scheme: least-used
Channel number: both

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The longest-idle hunt schemes attempts to route a call using a channel from the trunk group member that has been idle for the longest time.

If the **even** qualifier is set, the search looks for an even-numbered idle channel from the trunk group member that has been idle the longest. If no even-numbered idle channel is found, the search looks for an odd-numbered idle channel from the trunk group member that has the shortest idle time.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel from the trunk group member that has been idle the longest. If no odd-numbered idle channel is found, the search looks for an even-numbered idle channel from the trunk group member that has the shortest idle time.

If the **both** qualifier is set, the search looks for any (odd or even) idle channel in the trunk group member that has been idle the longest.

If no channel is available in any of the trunk group members, the software returns the standard “no service” message.

Examples

The following example searches in ascending order for an even-numbered idle channel in the trunk group member having the largest idle time:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme longest-idle even
```

Related Commands

Command	Description
hunt-scheme least-idle	Enables the least-idle hunt scheme.
trunk group	Initiates a trunk group profile.

hunt-scheme random

To enable the random search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme random** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme random

no hunt-scheme

Syntax Description

This command has no arguments or keywords.

Command Default

Hunt scheme: least-used

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The random search method selects trunk group member at random for an idle channel. After the trunk group member is selected, a channel is chosen at random. If that channel is not available, another trunk group member is chosen at random, and one of its channels is randomly chosen.

If no channel is available, the software returns the standard “no service” message.

Examples

The following example searches trunk group members in random order for an idle channel:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme random
```

Related Commands

Command	Description
trunk group	Initiates a trunk group profile.

hunt-scheme round-robin

To enable the round robin search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme round-robin [**both | even | odd** [**up | down**]]

no hunt-scheme

Syntax Description

both	Searches for an idle channel among both even- and odd-numbered channels at the same precedence.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is used.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is used.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used
Channel number: both

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The round-robin hunt scheme searches trunk group members one after the other for an idle channel. The history of the most recently used trunk group member is saved to identify the next trunk group member to use for a new idle channel request. This method tries to balance the load of channel use across trunk group members.

For example, suppose a trunk group has three trunk group members: A, B, and C. Trunk group member A has the highest preference, B has the next highest, and C has the lowest. The software starts the search with A:

- If A has an idle channel, that channel is used, and the next request for an idle channel starts with B.
- If A does not have an idle channel, the search moves to B:
- If B has an idle channel, that channel is used, and the next request for an idle channel starts with C.
- If B does not have an idle channel, the search moves to C:

- If C has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If C does not have an idle channel, the search returns to A.

If none of the trunk group members has an idle channel available for the current channel request, the software returns the standard "no service" message.

Compare this hunt scheme with **hunt-scheme sequential**, in which the next request for an idle channel always starts with the first trunk group member of the trunk group, regardless of where the last idle channel was found.

If the **even** qualifier is set, the search looks for an even-numbered idle channel starting with the trunk group member having the highest preference. If no even-numbered idle channel is found, the search looks for an even-numbered idle channel in the next trunk group member. If no even-numbered idle channel is found in any trunk group member, the search repeats the process for an odd-numbered channel.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel, and if none is found in any of the trunk group members, the search repeats the process for an even-numbered channel.

If the **both** qualifier is set, the search looks for any idle channel in the trunk group member.

Examples

The following example searches for an even-numbered idle channel starting with the trunk group member next in order after the previously used member:

```
Router(config)# trunk group northwestregion
Router(config-trunk-group)# hunt-scheme round-robin even
```

Related Commands

Command	Description
hunt-scheme sequential	Enables a "sequential idle channel" hunt scheme.
trunk group	Initiates a trunk group profile definition.

hunt-scheme sequential

To specify the sequential search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme sequential** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme sequential [**both** | **even** | **odd** [**up** | **down**]]

no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used
Channel number: both
Direction: up

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The sequential hunt scheme selects an idle channel, starting with the trunk group member that has the highest preference within the trunk group. Regardless of where the last idle channel was found, an idle channel request starts searching with this highest-preference trunk group member.

For example, suppose a trunk group has three trunk group members: A, B, and C. Trunk group member A has the highest preference, B has the next highest, and C has the lowest. The software starts the search with trunk group A:

- If A has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If A does not have an idle channel, the search moves to B:
- If B has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If B does not have an idle channel, the search moves to C:
- If C has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If C does not have an idle channel, the software returns the standard “no service” message.

Compare this hunt scheme with **hunt-scheme round-robin**, where the next request for an idle channel starts with the next unused trunk group member of the trunk group.

If the **even** qualifier is set, the search looks for an even-numbered idle channel starting with the trunk group member having the highest preference. If no even-numbered idle channel is found, the search looks for an even-numbered idle channel in the next trunk group member. If no even-numbered idle channel is found, the search repeats the process for an odd-numbered idle channel.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel, starting with the trunk group member having the highest preference. If none is found in any of the trunk group members, the search repeats the process for an even-numbered channel.

If the **both** qualifier is set, the search looks for any idle channel in the trunk group member.

Use the sequential hunt scheme in situations that benefit from a predictable channel allocation. In addition, if one end of the routing path is defined with **sequential even up** and the other end with **sequential odd up**, glare conditions are avoided.

Examples

The following example searches in ascending order for an even-numbered idle channel starting with the trunk group member of highest precedence:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme sequential even up
```

Related Commands

Command	Description
hunt-scheme round-robin	Enables a round-robin hunt scheme.
trunk group	Initiates a trunk group profile definition.

huntstop

To disable all dial-peer hunting if a call fails when using hunt groups, use the **huntstop** command in dial peer configuration mode. To reenable dial-peer hunting, use the **no** form of this command.

huntstop

no huntstop

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Once you enter this command, no further hunting is allowed if a call fails on the specified dial peer.

Note This command can be used with all types of dial peers.

Examples The following example shows how to disable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
 huntstop
```

The following example shows how to reenable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
 no huntstop
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.

Cisco IOS Voice Commands: I

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

icpif

To specify the Calculated Planning Impairment Factor (ICPIF) for calls sent by a dial peer, use the **icpif** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

icpif *number*

no icpif

Syntax Description

number	Integer, expressed in equipment impairment factor units, that specifies the ICPIF value. Range is 0 to 55. The default is 20.

Command Default

20

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	The *number* default value for this command was changed from 30 to 20.

Usage Guidelines

This command is applicable only to VoIP dial peers.

Use this command to specify the maximum acceptable impairment factor for the voice calls sent by the selected dial peer.

Examples

The following example disables the **icpif** command:

```
dial-peer voice 10 voip
 icpif 0
```

id

To configure the local identification (ID) for a neighboring border element (BE), use the **id** command in Annex G neighbor border element (BE) configuration mode. To remove the local ID, use the **no** form of this command.

id *neighbor-id*

no id *neighbor-id*

Syntax Description

neighbor-id	ID for a neighboring BE. The identification ID must be an International Alphabet 5 (IA5) string and cannot include spaces. This identifier is local and is not related to the border element ID.

Defaults

No default behavior or values

Command Modes

Annex G neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example configures the local ID for a neighboring BE. The identifier is 2333.

```
Router(config-annexg-neigh)# id 2333
```

The following example shows the the error response when an undefined neighbor ID is entered:

```
Router(config-annexg-neigh)#no id def
% Entry not valid, id not configured.

To deconfigure id under different neighbor you have to expilicitly go into that neighbor
and deconfigure the id.
```

Related Commands

Command	Description
advertise (annex G)	Controls the type of descriptors that the BE advertises to its neighbors.
port	Configures the port number of the neighbor that is used for exchanging Annex G messages.
query-interval	Configures the interval at which the local BE queries the neighboring BE.

idle-voltage

To specify the idle voltage on an Foreign Exchange Station (FXS) voice port, use the **idle-voltage** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

idle-voltage {**high** | **low**}

no idle-voltage

Syntax Description

high	The talk-battery (tip-to-ring) voltage is high (–48V) when the FXS port is idle.
low	The talk-battery (tip-to-ring) voltage is low (–24V) when the FXS port is idle.

Command Default

The idle voltage is –24V

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco MC3810.

Usage Guidelines

Some fax equipment and answering machines require a –48V idle voltage to be able to detect an off-hook condition in a parallel phone.

If the idle voltage setting is **high**, the talk battery reverts to –24V whenever the voice port is active (off hook).

Examples

The following example sets the idle voltage to –48V on voice port 1/1:

```
voice-port 1/1
 idle-voltage high
```

The following example restores the default idle voltage (–24V) on voice port 1/1:

```
voice-port 1/1
 no idle-voltage
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

ignore

To configure the North American E&M or E&M MELCAS voice port to ignore specific receive bits, use the **ignore** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

ignore {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}

no ignore {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}

Syntax Description

rx-a-bit	Ignores the receive A bit.
rx-b-bit	Ignores the receive B bit.
rx-c-bit	Ignores the receive C bit.
rx-d-bit	Ignores the receive D bit.

Command Default

The default is mode-dependent:

- North American E&M:
  - The receive B, C, and D bits are ignored
  - The receive A bit is not ignored
- E&M MELCAS:
  - The receive A bit is ignored
  - The receive B, C, and D bits are not ignored

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **ignore** command applies to E&M digital voice ports associated with T1/E1 controllers. Repeat the command for each receive bit to be configured. Use this command with the **define** command.

Examples

To configure voice port 1/1 to ignore receive bits A, B, and C and to monitor receive bit D, enter the following commands:

```
voice-port 1/1
 ignore rx-a-bit
 ignore rx-b-bit
 ignore rx-c-bit
 no ignore rx-d-bit
```

To configure voice port 1/0/0 to ignore receive bits A, C, and D and to monitor receive bit B, enter the following commands:

```
voice-port 1/0/0
 ignore rx-a-bit
 ignore rx-c-bit
 ignore rx-d-bit
 no ignore rx-b-bit
```

Related Commands

Command	Description
condition	Manipulates the signaling bit pattern for all voice signaling types.
define	Defines the transmit and receive bits for North American E&M and E&M MELCAS voice signaling.
show voice port	Displays configuration information for voice ports.

ignore (interface)

To configure the serial interface to ignore the specified serial signals as the line up/down indicator, use the **ignore** command in interface configuration mode. To restore the default, use the **no** form of this command.

DCE Asynchronous Mode

ignore [dtr | rts]

no ignore [dtr | rts]

DCE Synchronous Mode

ignore [dtr | local-loopback | rts]

no ignore [dtr | local-loopback | rts]

DTE Asynchronous Mode

ignore [cts | dsr]

no ignore [cts | dsr]

DTE Synchronous Mode

ignore [cts | dcd | dsr]

no ignore [cts | dcd | dsr]

Syntax Description

dtr	Specifies that the DCE ignores the Data Terminal Ready (DTR) signal.
rts	Specifies that the DCE ignores the Request To Send (RTS) signal.
local-loopback	Specifies that the DCE ignores the local loopback signal.
cts	Specifies that the DTE ignores the Clear To Send (CTS) signal.
dsr	Specifies that the DTE ignores the Data Set Ready (DSR) signal.
dcd	Specifies that the DTE ignores the Data Carrier Detect (DCD) signal.

Command Default

The **no** form of this command is the default. The serial interface monitors the serial signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as a Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to ignore the DCD signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore dcd
```

Related Commands

Command	Description
debug serial lead-transition	Activates the leads status transition debug capability for all capable ports.
show interfaces serial	Displays information about a serial interface.

image encoding

To specify an encoding method for fax images associated with a Multimedia Mail over IP (MMoIP) dial peer, use the **image encoding** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

image encoding {**mh** | **mr** | **mmr** | **passthrough**}

no image encoding {**mh** | **mr** | **mmr** | **passthrough**}

Syntax Description

mh	Modified Huffman image encoding. This is the IETF standard.
mr	Modified Read image encoding.
mmr	Modified Modified Read image encoding.
passthrough	The image is not modified by an encoding method.

Command Default Passthrough encoding

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Use this command to specify an encoding method for e-mail fax TIFF images for a specific MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image encoding value for that off-ramp call leg, store-and-forward fax ignores the off-ramp MMoIP setting and sends the file using Modified Huffman encoding.

There are four available encoding methods:

- Modified Huffman (MH)—One-dimensional data compression scheme that compresses data in only one direction (horizontal). Modified Huffman compression does not allow the transmission of redundant data. This encoding method produces the largest image file size.
- Modified Read (MR)—Two-dimensional data compression scheme (used by fax devices) that handles the data compression of the vertical line and that concentrates on the space between lines and within given characters.

- Modified Modified Read (MMR)—Data compression scheme used by newer Group 3 fax devices. This encoding method produces the smallest possible image file size and is slightly more efficient than Modified Read.
- Passthrough—No encoding method is applied to the image—meaning that the image is encoded by whatever encoding method is used by the fax device.

The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. RFC 2301 requires that compliant receivers support TIFF images with MH encoding and fine or standard resolution. If a receiver supports features beyond this minimal requirement, you might want to configure the Cisco AS5300 universal access server to send enhanced-quality documents to that receiver.

The primary reason to use a different encoding scheme from MH is to save network bandwidth. MH ensures interoperability with all Internet fax devices, but it is the least efficient of the encoding schemes for sending fax TIFF images. For most images, MR is more efficient than MH, and MMR is more efficient than MR. If you know that the recipient is capable of receiving more efficient encodings than just MH, store-and-forward fax allows you to send the most efficient encoding that the recipient can process. For end-to-end closed networks, you can choose any encoding scheme because the off-ramp gateway can process MH, MR, and MMR.

Another factor to consider is the viewing software. Many viewing applications (for example, those that come with Windows 95 or Windows NT) are able to display MH, MR, and MMR. Therefore you should decide, on the basis of the viewing application and the available bandwidth, which encoding scheme is right for your network.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example selects Modified Modified Read as the encoding method for fax TIFF images sent by MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 image encoding mmr
```

Related Commands

Command	Description
image resolution	Specifies a particular fax image resolution for a specific MMoIP dial peer.

image resolution

To specify a particular fax image resolution for a specific multimedia mail over IP (MMoIP) dial peer, use the **image resolution** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

image resolution {**fine | standard | superfine | passthrough**}

no image resolution {**fine | standard | superfine | passthrough**}

Syntax Description

fine	Configures the fax TIFF image resolution to be 204-by-196 pixels per inch.
standard	Configures the fax TIFF image resolution to be 204-by-98 pixels per inch.
superfine	Configures the fax TIFF image resolution to be 204-by-391 pixels per inch.
passthrough	Indicates that the resolution of the fax TIFF image is not altered.

Command Default

passthrough

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600, Cisco 3600, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to specify a resolution (in pixels per inch) for e-mail fax TIFF images sent by the specified MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image resolution value for that off-ramp call leg, store-and-forward fax ignores the off-ramp MMoIP setting and sends the file using fine resolution.

This command enables you to increase or decrease the resolution of a fax TIFF image, thereby changing not only the resolution but also the size of the fax TIFF file. The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. The primary reason to configure a different resolution is to save network bandwidth.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example selects fine resolution (204-by-196 pixels per inch) for e-mail fax TIFF images associated with MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 image encoding mh
 image resolution fine
```

Related Commands

Command	Description
image encoding	Specifies an encoding method for fax images associated with an MMoIP dial peer.

impedance

To specify the terminating impedance of a voice-port interface, use the **impedance** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

impedance {**600c** | **600r** | **900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}

no impedance {**600c** | **600r** | **900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}

Syntax Description

600c	600 ohms + 2.15uF[1].
600r	Resistive 600-ohm termination.
900c	900 ohms + 2.15uF[1].
900r	Resistive 900-ohm termination.
complex1	220 ohms + (820 ohms || 115 nF)[1].
complex2	270 ohms + (750 ohms || 150 nF)[1].
complex3	370 ohms + (620 ohms || 310 nF)[1].
complex4	600r, line = 270 ohms + (750 ohms || 150 nF)[1].
complex5	320 + (1050 ohms || 230 nF), line = 12 Kft[1].
complex6	600r, line = 350 + (1000 ohms || 210 nF)[1].

1. The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.

Note This table represents the full set of impedances. Not all modules support the full set of impedance values shown here. To determine which impedance values are available on your modules, enter impedance ? in the command-line interface to see a list of the values you can configure.

Command Default 600r

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T and support was added for the **complex3**, **complex4**, **complex5**, and **complex6** keywords on the Cisco 2600XM series, Cisco 2691, Cisco 2800 series, Cisco 3662 (telco models), Cisco 3700 series, and Cisco 3800 series.

Usage Guidelines

Use this command to specify the terminating impedance of analog telephony interfaces. The impedance value must match the specifications from the telephony system to which it is connected. Different countries often have different standards for impedance. CO switches in the United States are predominantly 600r. PBXs in the United States are 600r or 900c.

If the impedance is set incorrectly (if there is an impedance mismatch), a significant amount of echo is generated (which could be masked if the **echo-cancel** command has been enabled). In addition, gains might not work correctly if there is an impedance mismatch.

Configuring the impedance on a voice port changes the impedance on both voice ports of a VPM card. This voice port must be shut down and then opened for the new value to take effect.

Examples

The following example configures an FXO voice port on the Cisco 3600 series router for an impedance of 600 ohms (real):

```
voice-port 1/0/0
impedance 600r
shutdown/no shutdown
```

The following example configures an E&M voice port on a Cisco 2800 for an impedance of complex3:

```
voice-port 1/1
impedance complex3
shutdown/no shutdown
```

Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.
echo-cancel enable	Enables the cancellation of voice that is sent out the interface and received back on the same interface.

inband-alerting

To enable inband alerting, use the **inband-alerting** command in the SIP user agent configuration mode. To disable inband alerting, use the **no** form of this command.

inband-alerting

no inband-alerting

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(3)T	This command was limited to enabling and disabling inband alerting.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If inband alerting is enabled, the originating gateway can open an early media path (upon receiving a 180 or 183 message with a SDP body). Inband alerting allows the terminating gateway or switch to feed tones or announcements before a call is connected. If inband alerting is disabled, local alerting is generated on the originating gateway.

To reset this command to the default value, use the **default** command.

Examples

The following example disables inband alerting:

```
Router(config)# sip-ua
Router(config-sip-ua)# no inband-alerting
```

Related Commands

Command	Description
default	Sets a command to its default.
exit	Exits the SIP user agent configuration mode.
max-forwards	Specifies the maximum number of hops for a request.
no	Negates a command or set its defaults.
retry	Configures the SIP signaling timers for retry attempts.

Command	Description
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

inbound ttl

To set the inbound time-to-live value, use the **inbound ttl** command in Annex G neighbor service configuration mode. To reset to the default, use the **no** form of this command.

inbound ttl *ttl-value*

no inbound ttl

Syntax Description

ttl-value	Inbound time-to-live (TTL) value, in seconds. Range is 0 to 2147483. When set to 0, the service relationship does not expire. The default is 120.

Defaults

120 seconds

Command Modes

Annex G neighbor service configuration (config-nxg-neigh-svc)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Service relationships are defined to be unidirectional. Establishing a service relationship between border element A and border element B entitles A to send requests to B and expect responses. For B to send requests to A and expect responses, a second service relationship must be established. From A's perspective, the service relationship that B establishes with A is designated the "inbound" service relationship. Use this command to indicate the duration of the relationship between border elements that participate in a service relationship.

Examples

The following example sets the inbound time-to-live value to 420 seconds (7 minutes):

```
Router(config-nxg-neigh-svc)# inbound ttl 420
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time that a border element attempts delivery.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.

incoming alerting

To instruct an FXO ground-start voice port to modify its means of detecting an incoming call, use the **incoming alerting** command in voice-port configuration mode. To return to the default call detection method, use the **no** form of this command.

incoming alerting {**ring-only**}

no incoming alerting

Syntax Description

ring-only	Count incoming rings to detect incoming calls to the voice port that should be answered by the router.

Command Default

The FXO ground-start voice port detects an incoming call either by detecting the ring voltage applied to the line by the PSTN central office (CO) or by detecting that tip-ground is present for greater than about 7 seconds.

Command Modes

Voice-port configuration

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.

Usage Guidelines

This command is valid only on FXO ports that have been configured with the **signal ground-start** command.

This command is necessary when two Cisco Unified CallManager Express (Cisco Unified CME) routers are used to provide redundant failover for incoming PSTN FXO ground-start lines. The voice ports for these trunk lines are wired in parallel between the two routers. The primary router is set to answer incoming calls after the first ring by default. The secondary router is set to answer incoming calls after 2 or 3 rings using the **ring number** command in voice-port configuration mode. As long as the primary router is operating, then the secondary router will not see enough rings to trigger it to answer the call. When the primary router is not operating, the secondary router has to be able to detect incoming ring signals so that it can answer calls. The default method of incoming call detection is not appropriate for voice ports on a secondary Cisco Unified CME router. The **incoming alerting ring-only** command must be used to modify the incoming call detection logic so that the voice port counts the number of incoming call rings instead of using the default call detection method.

Examples

The following example sets ring-only as the detection method for incoming calls on voice port 3/0/0, which is an FXO ground-start voice port.

```
Router(config)# voice-port 3/0/0
Router(config-voiceport)# signal ground-start
Router(config-voiceport)# incoming alerting ring-only
```

Related Commands

Command	Description
ring number	Specifies the maximum number of rings to be detected before an incoming call is answered by the router.
signal	Specifies the type of signaling for a voice port.

incoming called-number (call filter match list)

To configure debug filtering for incoming called numbers, use the **incoming called-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming called-number [**+**]*string*[**T**]

no incoming called-number [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match incoming called number 5550123:

```
call filter match-list 1 voice
 incoming called-number 5550123
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming called-number (dial peer)

To specify a digit string that can be matched by an incoming call to associate the call with a dial peer, use the **incoming called-number** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

incoming called-number [**+**]*string*[**T**]

no incoming called-number [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the destination-pattern value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default No incoming called number is defined

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3NA	This command was implemented on the Cisco AS5800.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines When a Cisco device is handling both modem and voice calls, it needs to be able to identify the service type of the call—meaning whether the incoming call to the server is a modem or a voice call. When the access server handles only modem calls, the service type identification is handled through modem pools. Modem pools associate calls with modem resources based on the dialed number identification service (DNIS). In a mixed environment, in which the server receives both modem and voice calls, you need to identify the service type of a call by using this command.

If you do not use this command, the server attempts to resolve whether an incoming call is a modem or voice call on the basis of the interface over which the call arrives. If the call comes in over an interface associated with a modem pool, the call is assumed to be a modem call; if a call comes in over a voice port associated with a dial peer, the call is assumed to be a voice call.

By default, there is no called number associated with the dial peer, which means that incoming calls are associated with dial peers by matching calling number with answer address, call number with destination pattern, or calling interface with configured interface.

Use this command to define the destination telephone number for a particular dial peer. For the on-ramp POTS dial peer, this telephone number is the DNIS number of the incoming fax call. For the off-ramp MMoIP dial peer, this telephone number is the telephone number of the destination fax machine.

This command applies to both VoIP and POTS dial peers and to on-ramp and off-ramp store-and-forward fax functions.

This command is also used to provide a matching VoIP dial peer on the basis of called number when fax or modem pass-through with named signaling events (NSEs) is defined globally on a terminating gateway.

You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number.
```

Examples

The following example configures calls that come into the router with a called number of 555-0163 as being voice calls:

```
dial peer voice 10 pots
 incoming called-number 5550163
```

The following example sets the number (310) 555-0142 as the incoming called number for MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 incoming called-number 3105550142
```

incoming calling-number (call filter match list)

To configure debug filtering for incoming calling numbers, use the **incoming calling-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming calling-number [**+**]*string*[**T**]

no incoming calling-number [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match incoming calling number 5550125:

```
call filter match-list 1 voice
 incoming calling-number 5550125
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming dialpeer

To configure debug filtering for the incoming dial peer, use the **incoming dialpeer** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming dialpeer *tag*

no incoming dialpeer *tag*

Syntax Description

tag	Digits that define a specific dial peer. Valid entries are 1 to 2,147,483,647.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match incoming dial peer 12:

```
call filter match-list 1 voice
 incoming dialpeer 12
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming port	Configure debug filtering for the incoming port.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming media local ipv4

To configure debug filtering for the incoming media local IPv4 addresses for the voice gateway receiving the media stream, use the **incoming media local ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming media local ipv4 *ip_address*

no incoming media local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match incoming media on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming media local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming media remote ipv4

To configure debug filtering for the incoming media remote IPv4 addresses for the voice gateway receiving the media stream, use the **incoming media remote ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming media remote ipv4 *ip_address*

no incoming media remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match incoming media on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming media remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming port

To configure debug filtering for the incoming port, use the **incoming port** command in call filter match list configuration mode. To disable, use the **no** form of this command.

Cisco 2600, Cisco 3600, and Cisco 3700 Series

incoming port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

no incoming port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

Cisco 2600 and Cisco 3600 Series with a High-Density Analog Network Module (NM-HDA)

incoming port {*slot-number*/*subunit-number*/*port*}

no incoming port {*slot-number*/*subunit-number*/*port*}

Cisco AS5300

incoming port *controller-number*:**D**

no incoming port *controller-number*:**D**

Cisco AS5400

incoming port *card*/*port*:**D**

no incoming port *card*/*port*:**D**

Cisco AS5800

incoming port {*shelf*/*slot*/*port*:**D** | *shelf*/*slot*/*parent*:*port*:**D**}

no incoming port {*shelf*/*slot*/*port*:**D** | *shelf*/*slot*/*parent*:*port*:**D**}

Cisco MC3810

incoming port *slot*/*port*

no incoming port *slot*/*port*

Syntax Description

Cisco 2600, Cisco 3600 Series and Cisco 3700 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
port	Voice port number. Valid entries are 0 and 1.
slot	The router location in which the voice port adapter is installed. Valid entries are 0 to 3.

port:	Indicates the voice interface card location. Valid entries are 0 and 3.
ds0-group-no	Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300

controller-number	T1 or E1 controller.
:D	D channel associated with ISDN PRI.

Cisco AS5400

card	Specifies the T1 or E1 card. Valid entries for the *card* argument are 1 to 7.
port	Specifies the voice port number. Valid entries are 0 to 7.
:D	Indicates the D channel associated with ISDN PRI.

Cisco AS5800

shelf	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *shelf* argument are 0 to 9999.
slot	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *slot* argument are 0 to 11.
port	Specifies the voice port number. • T1 or E1 controller on the T1 card —Valid entries are 0 to 11. • T1 controller on the T3 card—Valid entries are 1 to 28.
:*port*	Specifies the value for the *parent* argument. The valid entry is 0.
:D	Indicates the D channel associated with ISDN PRI.

Cisco MC3810

slot	The *slot* argument specifies the number slot in the router in which the VIC is installed. The only valid entry is 1.
port	The *port* variable specifies the voice port number. Valid interface ranges are as follows: • T1—ANSI T1.403 (1989), Telcordia TR-54016. • E1— ITU G.703. • Analog Voice—Up to six ports (FXS, FXO, E & M). • Digital Voice— Single T1/E1 with cross-connect drop and insert, CAS and CCS signaling, PRI QSIG. • Ethernet—Single 10BASE-T. • Serial—Two five-in-one synchronous serial (ANSI EIA/TA-530, EIA/TA-232, EIA/TA-449; ITU V.35, X.21, Bisync, Polled async).

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match incoming port 1/1/1 on a Cisco 3660 voice gateway:

```
call filter match-list 1 voice
 incoming port 1/1/1
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming secondary-called-number

To configure debug filtering for incoming called numbers from the second stage of a two-stage scenario, use the **incoming secondary-called-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming secondary-called-number *string*

no incoming secondary-called-number *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range. • Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Two-stage dialing occurs when the voice gateway presents a dial-tone before accepting digits. When a voice call comes into the Cisco IOS voice gateway, the voice port on the router is seized inbound by a PBX or CO switch. The voice gateway then presents a dial tone to the caller and collects digits until it can identify an outbound dial-peer. Dial-peer matching is done digit-by-digit whether the digits are dialed with irregular intervals by humans or in a regular fashion by telephony equipment sending the precollected digits. The voice gateway attempts to match a dial-peer after each digit is received.

Examples The following example shows the voice call debug filter set to match incoming secondary called number 8288807:

```
call filter match-list 1 voice
 incoming secondary-called-number 8288807
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming signaling local ipv4

To configure debug filtering for the incoming signaling local IPv4 addresses for the gatekeeper managing the signaling, use the **incoming signaling local ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming signaling local ipv4 *ip_address*

no incoming signaling local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match incoming signaling on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming signaling local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

incoming signaling remote ipv4

To configure debug filtering for the incoming signaling remote IPv4 addresses for the gatekeeper managing the signaling, use the **incoming signaling remote ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming signaling remote ipv4 *ip_address*

no incoming signaling remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match incoming signaling on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming signaling remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

incoming uri

To specify the voice class used to match a VoIP dial peer to the uniform resource identifier (URI) of an incoming call, use the **incoming uri** command in dial peer voice configuration mode. To remove the URI voice class from the dial peer, use the **no** form of this command.

H.323 Session Protocol

incoming uri {**called** | **calling**} *tag*

no incoming uri {**called** | **calling**}

Session Initiation Protocol (SIP) Session Protocol

incoming uri {**from** | **request** | **to** | **via**} *tag*

no incoming uri {**from** | **request** | **to** | **via**}

Syntax Description

called	Destination URI in the H.225 message of an H.323 call.
calling	Source URI in the H.225 message of an H.323 call.
tag	Alphanumeric label that uniquely identifies the voice class. This *tag* argument must be configured with the **voice class uri** command.
from	From header in an incoming SIP Invite message.
request	Request-URI in an incoming SIP Invite message.
to	To header in an incoming SIP Invite message.
via	Via header in an incoming SIP Invite message.

Command Default

No voice class is specified.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The **via** keyword was included.

Usage Guidelines

- Before you use this command, configure the voice class by using the **voice class uri** command.
- The keywords depend on whether the dial peer is configured for SIP with the **session protocol sipv2** command. The **from**, **request**, **to**, and **via** keywords are available only for SIP dial peers. The **called** and **calling** keywords are available only for dial peers using H.323.

- This command applies rules for dial peer matching. Table 29 and Table 30 show the rules and the order in which they are applied when the **incoming uri** command is used. The gateway compares the dial-peer command to the call parameter in its search to match an inbound call to a dial peer. All dial peers are searched based on the first match criterion. Only if no match is found does the gateway move on to the next criterion.

Table 29 Dial-Peer Matching Rules for Inbound URI in SIP Calls

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri via**	Via URI
2	**incoming uri request**	Request-URI
3	**incoming uri to**	To URI
4	**incoming uri from**	From URI
5	**incoming called-number**	Called number
6	**answer-address**	Calling number
7	**destination-pattern**	Calling number
8	**carrier-id source**	Carrier-ID associated with the call

Table 30 Dial-Peer Matching Rules for Inbound URI in H.323 Calls

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri called**	Destination URI in H.225 message
2	**incoming uri calling**	Source URI in H.225 message
3	**incoming called-number**	Called number
4	**answer-address**	Calling number
5	**destination-pattern**	Calling number
6	**carrier-id source**	Source carrier-ID associated with the call

Note Calls using an E.164 number, rather than a URI, use the dial-peer matching rules that existed prior to Cisco IOS Release 15.1(2)T. For information, see the*Dial Peer Configuration on Voice Gateway Routers* document, Cisco IOS Voice Configuration Library.

- You can use this command multiple times in the same dial peer with different keywords. For example, you can use **incoming uri called** and **incoming uri calling** in the same dial peer. The gateway then selects the dial peer based on the matching rules described in Table 29 and Table 30.

Examples

The following example matches on the destination telephone URI in incoming H.323 calls by using the ab100 voice class:

```
dial-peer voice 100 voip
 incoming uri called ab100
```

The following example matches on the incoming via URI for SIP calls by using the ab100 voice class:

```
dial-peer voice 100 voip
 session protocol sipv2
 incoming uri via ab100
```

Related Commands

Command	Description
answer-address	Specifies the calling number to match for a dial peer.
debug voice uri	Displays debugging messages related to URI voice classes.
destination-pattern	Specifies the telephone number to match for a dial peer.
dial-peer voice	Enters dial peer voice configuration mode to create or modify a dial peer.
incoming called-number	Specifies the incoming called number matched to a dial peer.
session protocol	Specifies the session protocol in the dial peer for calls between the local and remote router.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

index (voice class)

To define one or more numbers for a voice class called number, or a range of numbers for a voice class called number pool, use the **index** command in voice class configuration mode. To remove the number or range of numbers, use the **no** form of this command.

index *number called-number*

no index *number called-number*

Syntax Description

number	Digits that identify this index. Range is 1 to 2147483647.
called-number	Specifies a called number, or a range of called numbers, in E.164 format.

Command Default No index is configured.

Command Modes Voice class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to define one or more numbers for a voice class called number, or a range of numbers for a voice class called number pool. You can define multiple indexes for any inbound or outbound voice class called number or voice class called number pool.

When defining a range of numbers for a called number pool:

- The range of numbers must be in E.164 format.
- The beginning number and ending number must be the same length.
- The last digit of each number must be 0 to 9.
- Leading '+' (if used) must be defined from in the range of called numbers.

Examples The following example shows the configuration for indexes in voice class called number pool 100:

```
voice class called number pool 100
 index 1 4085550100 - 4085550111 (Range of called numbers are 4085550100 up to 4085550111)
 index 2 +3227045000
```

The following example shows configuration for indexes in voice class called number outbound 222:

```
voice class called number outbound 222
 index 1 4085550101
 index 2 4085550102
 index 2 4085550103
```

Related Commands

Command	Description
voice class called number	One or more called numbers configured for a voice class.

info-digits

To automatically prepend two information digits to the beginning of a dialed number associated with the given POTS dial peer, use the **info-digits** command in dial-peer configuration mode. To prepend the info-digits with "00" use the **default info-digits** form of this command. To keep the router from automatically prepending the two-digit information numbers to the beginning of the POTS dial peer, use the **no** form of this command.

info-digits *xx*

default info-digits

no info-digits

Syntax Description

xx	Specifies the two-digit prefix that the router will automatically prepend to the dialed number for the given POTS dial peer to identify the origin of the call. This value cannot contain any more or less than two digits. Valid values include: • 00—Regular line • 01—4- and 8-party • 06—Hotel or Motel • 07—Coinless • 10—Test call • 27—Coin • 95—Test call **Note** Values 12 through 19 cannot be assigned because of conflicts with international 20 Automatic Identification of Outward listed directory number sent.

Defaults

The dialed number is prepended with "00", indicating that the dialed number is a regular line.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.2(1)T	This command was introduced.
12.3(7)T	This command was modified. The default behavior was changed to prepend the dialed number the with "00".

Usage Guidelines

This command is designed to prepend a pair of information digits to the beginning of the dialed number string for the POTS dial peer that will enable you to dynamically redirect the outgoing call. The **info-digits** command is only available for POTS dial peers tied to a voice-port that corresponds to Feature Group-D (FGD) Exchange Access North American (EANA) signaling that provides specific call services such as emergency 911 calls in the United States. Configuring the info-digit command for other voice-port types is not advised and may yield undesirable results.

Examples

The following example prepends the information number string 91 to the beginning of the dialed number for POTS dial peer 10:

```
dial-peer voice 10 pots
 info-digits 91
```

information-type

To select a specific information type for a Voice over IP (VoIP) or plain old telephone service (POTS) dial peer, use the **information-type** command in dial peer configuration mode. To remove the current information type setting, use the **no** form of this command. To return to the default configuration, use the **no** form of this command.

information-type {**fax** | **voice** | **video**}

no information-type

Syntax Description

fax	The information type is set to store-and-forward fax.
voice	The information type is set to voice. This is the default.
video	The information type is set to video.

Command Default Voice

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.4(11)T	The **video** keyword was added.

Usage Guidelines The **fax** keyword applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples The following example shows the configuration for information type fax for VoIP dial peer 10:

```
dial-peer voice 10 voip
 information-type fax
```

The following example shows the configuration for information type video for POTS dial peer 22:

```
dial-peer voice 22 pots
 information-type video
```

Related Commands

Command	Description
isdn integrate calltype all	Enables integrated mode (for data, voice, and video) on ISDN BRI or PRI interfaces.

inject guard-tone

To play out a guard tone with the voice packet, use the **inject guard-tone** command in voice-class configuration mode. To remove the guard tone, use the **no** form of this command.

inject guard-tone *frequency amplitude* [**idle**]

no inject guard-tone *frequency amplitude* [**idle**]

Syntax Description

frequency	Frequency, in Hz, of the tone to be injected. Range is integers from 1 to 4000.
amplitude	Amplitude, in dBm, of the tone to be injected. Range is integers from –50 to –3.
idle	(Optional) Play out the inverse of the guard tone when there are no voice packets. Idle tone and guard tone are mutually exclusive.

Command Default

No guard tone is injected.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **inject guard-tone** command has an effect on an ear and mouth (E&M) analog or digital voice port only if the signal type for that port is Land Mobile Radio (LMR). The guard tone is played out with the voice packet to keep the radio channel up. Guard tones of 1950 Hz and 2175 Hz can be filtered out before the voice packet is sent from the digital signal processor (DSP) to the network using the **digital-filter** command.

Examples

The following example configures a guard tone of 1950 Hz and –10 dBm to be played out with voice packets:

```
voice class tone-signal tone1
 inject guard-tone 2175 -30
```

Related Commands

Command	Description
digital-filter	Specifies the digital filter to be used before the voice packet is sent from the DSP to the network.

inject pause

To specify a pause between injected tones, use the **inject pause** command in voice-class configuration mode. To remove the pause, use the **no** form of this command.

inject pause *index milliseconds*

no inject pause *index milliseconds*

Syntax Description

index	Order of pauses and tones. Range is integers from 1 to 10.
milliseconds	Duration, in milliseconds, of the pause between injected tones. Range is integers from 10 to 500.

Command Default

milliseconds: 0 milliseconds

Command Modes

Voice-class configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **inject pause** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Use this command to specify the pause between injected tones specified with the **inject tone** command. Use the *index* argument of this command in conjunction with the *index* argument of the inject tone command to specify the order of the pauses and tones.

Examples

The following example configures a pause of 100 milliseconds after the injected tone:

```
voice class tone-signal 100
 inject tone 1 2000 0 200
 inject pause 2 100
```

Related Commands

Command	Description
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.

inject tone

To specify a wakeup or frequency selection tone to be played out before the voice packet, use the **inject tone** command in voice-class configuration mode. To remove the tone, use the **no** form of this command.

inject tone *index frequency amplitude duration*

no inject tone *index frequency amplitude duration*

Syntax Description

index	Order of pauses and tones. Range is integers from 1 to 10.
frequency	Frequency, in Hz, of the tone to be injected. Range is integers from 1 to 4000.
amplitude	Amplitude, in dBm, of the tone to be injected. Range is integers from –30 to 3.
duration	Duration, in milliseconds, of the tone to be injected. Range is integers from 10 to 500.

Command Default No tone is injected.

Command Modes Voice-class configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines The **inject tone** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Use this command with the **inject pause** command to configure wakeup and frequency selection tones. Use the *index* argument of this command in conjunction with the *index* argument of the **inject pause** command to specify the order of the pauses and tones.

If you configure injected tones with this command, be sure to use the **timing delay-voice tdm** command to configure a delay before the voice packet is played out. The delay must be equal to the sum of the durations of the injected tones and pauses in the tone-signal voice class.

Examples The following example configures a frequency selection tone to be played out before the voice packet:

```
voice class tone-signal 100
 inject tone 1 1950 3 150
 inject tone 2 2000 0 60
 inject pause 3 60
 inject tone 4 2175 3 150
 inject tone 5 1000 0 50
```

Related Commands

Command	Description
inject pause	Specifies a pause between injected tones.
timing delay-voice tdm	Specifies the delay before a voice packet is played out.

input gain

To configure a specific input gain value or enable automatic gain control, use the **input gain** command in voice-port configuration mode. To disable the selected amount of inserted gain, use the **no** form of this command.

input gain {*decibels* | **auto-control** [*auto-dbm*]}

no input gain {*decibels* | **auto-control** [*auto-dbm*]}

Syntax Description

decibels	Gain, in decibels (dB), to be inserted at the receiver side of the interface. Range is integers from –27 to 16. The default is 0.
auto-control	Enable automatic gain control.
auto-dbm	(Optional) Target speech level, in decibels per milliwatt (dBm), to be achieved at the receiver side of the interface. Range is integers from –30 to 3. The default is –9.

Command Default

decibels: 0 decibels
auto-dbm: –9 dBm

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels* argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	The **auto-control** keyword and *auto-dbm* argument were added.

Usage Guidelines

A system-wide loss plan must be implemented using both the **input gain** and **output attenuation** commands. You must consider other equipment (including PBXs) in the system when creating a loss plan. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there is typically a minimum attenuation of –6 dB between phones, especially if echo cancellers are present. Connections are implemented to provide 0 dB of attenuation when the **input gain** and **output attenuation** commands are configured with the default value of 0 dB.

You cannot increase the gain of a signal to the public switched telephone network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or increasing the output attenuation.

You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the **input gain** command.

Typical Land Mobile Radio (LMR) signaling systems send 0 dB out and expect –10 dB in. Setting output attenuation to 10 dB is typical. Output attenuation should be adjusted to provide the voice level required by the radio to produce correct transmitter modulation.

The **auto-control** keyword and *auto-dbm* argument are available on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **auto-control** keyword enables automatic gain control, which is performed by the digital signal processor (DSP). Automatic gain control adjusts speech to a comfortable volume when it becomes too loud or too soft. Because of radio network loss and other environmental factors, the speech level arriving at a router from an LMR system could be very low. You can use automatic gain control to ensure that the speech is played back at a more comfortable level. Because the gain is inserted digitally, the background noise can also be amplified. Automatic gain control is implemented as follows:

- Output level: –9 dB
- Gain range: –12 dB to 20 dB
- Attack time (low to high): 30 milliseconds
- Attack time (high to low): 8 seconds

Examples

The following example inserts a 3-dB gain at the receiver side of the interface in the Cisco 3600 series router:

```
port 1/0/0
 input gain 3
```

Related Commands

Command	Description
output attenuation	Configures a specific output attenuation value or enables automatic gain control for a voice port.

interface (RLM server)

To define the IP addresses of the Redundant Link Manager (RLM) server, use the **interface** command in interface configuration mode. To disable this function, use the **no** form of this command.

interface *name-tag*

no interface *name-tag*

Syntax Description

name-tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Command Default Disabled

Command Modes Interface configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines Each server can have multiple entries of IP addresses or aliases.

Examples The following example configures the access-server interfaces for RLM servers “Loopback1” and “Loopback2”:

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
 interface Loopback2
 ip address 10.1.1.2 255.255.255.255
rlm group 1
 server r1-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.

Command	Description
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

interface Dchannel

To specify an ISDN D-channel interface and enter interface configuration mode, use the **interface Dchannel** command in global configuration mode.

interface Dchannel *interface-number*

Syntax Description

interface-number	Specifies the ISDN interface number.

Note The *interface-number* argument depends on which controller the **rlm-group** subkeyword in the **pri-group timeslots** controller configuration command uses. For example, if the Redundant Link Manager (RLM) group is configured using the **controller e1 2/3** command, the D-channel interface command will be **interface Dchannel 2/3**.

Command Default No D-channel interface is specified.

Command Modes Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines This command is used specifically in Voice over IP (VoIP) applications that require release of the ISDN PRI signaling time slot for RLM configurations.

Examples The following example configures a D-channel interface for a Signaling System 7 (SS7)-enabled shared T1 link:

```
controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
 end

! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
 end
```

Related Commands

Command	Description
pri-group timeslots	Specifies an ISDN PRI group on a channelized T1 or E1 controller, and releases the ISDN PRI signaling time slot for environments that require that SS7-enabled VoIP applications share all slots in a PRI group.

interface event-log dump ftp

To enable the gateway to write the contents of the interface event log buffer to an external file, use the **interface event-log dump ftp** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log dump ftp *server*[**:***port]/file* **username** *username* **password** [*encryption-type*] *password*

no interface event-log dump ftp *server*[**:***port]/file* **username** *username* **password** [*encryption-type*] *password*

Syntax Description

server	Name or IP address of FTP server where the file is located.
port	(Optional) Specific port number on server.
file	Name and path of file.
username	Username required to access file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password	Password required to access file.

Command Default

Interface event log buffer is not written to an external file.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface event-log dump ftp** command.

Usage Guidelines

This command enables the gateway to automatically write the interface event log buffer to the named file when the buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **interface event-log max-buffer-size** command. To manually flush the event log buffer, use the **interface dump event-log** command in privileged EXEC mode.

Note

- Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:
- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Examples

The following example specifies that interface event log are written to an external file named int_elogs.log on a server named ftp-server:

```
application
    monitor
    interface event-log dump ftp ftp-server/elogs/int_elogs.log username myname password 0
    mypass
```

The following example specifies that application event logs are written to an external file named int_elogs.log on a server with the IP address of 10.10.10.101:

```
application
    monitor
    interface event-log dump ftp 10.10.10.101/elogs/int_elogs.log username myname password
    0 mypass
```

Related Commands

Command	Description
call application interface event-log dump ftp	Enable the gateway to write the contents of the interface event log buffer to an external file.
interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
interface event-log	Enables event logging for external interfaces used by voice applications.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface event-log error only

To restrict event logging to error events only for application interfaces, use the **interface event-log error-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log error-only

no interface event-log error-only

Syntax Description

This command has no arguments or keywords.

Command Default

All events are logged.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface event-log error only** command.

Usage Guidelines

This command limits the severity level of the events that are logged; it does not enable logging. You must use this command with the **interface event-log** command, which enables event logging for all application interfaces.

Examples

The following example enables event logging for error events only:

```
application
    monitor
    interface event-log error-only
```

Related Commands

Command	Description
call application interface event-log error-only	Restricts event logging to error events only for application interfaces.
interface event-log	Enables event logging for external interfaces used by voice applications.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface event-log max-buffer-size

To set the maximum size of the event log buffer for each application interface, use the **interface event-log max-buffer-size** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log max-buffer-size *kbytes*

no interface event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range is 1 to 10. Default is 4.

Command Default

4 KB

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface event-log max-buffer-size** command.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application interface** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **interface event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **interface event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Examples

The following example sets the maximum buffer size to 8 KB:

```
application
    monitor
    interface event-log max-buffer-size 8
```

Related Commands

Command	Description
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
interface event-log dump ftp	Enables the gateway to write the contents of the interface event log buffer to an external file.

Command	Description
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface max-server-records

To set the maximum number of application interface records that are saved, use the **interface max-server-records** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface max-server-records *number*

no interface max-server-records

Syntax Description		
	number	Maximum number of records to save. Range is 1 to 100. Default is 10.

Command Default 10

Command Modes Application configuration monitor

Command History	Release	Modification
	12.3(14)T	This command was introduced to replace the **call application interface max-server-records** command.

Usage Guidelines Only the specified number of records from the most recently accessed servers are kept.

Examples The following example sets the maximum saved records to 50:

```
application
    monitor
    interface max-server-records 50
```

Related Commands	Command	Description
	call application interface max-server-records	Sets the maximum number of application interface records that are saved.
	interface event-log	Enables event logging for external interfaces used by voice applications.
	interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
	show call application interface	Displays event logs and statistics for application interfaces.

interface stats

To enable statistics collection for application interfaces, use the **interface stats** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface stats

no interface stats

Syntax Description This command has no arguments or keywords.

Command Default Statistics collection is disabled.

Command Modes Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface stats** command.

Usage Guidelines To display the interface statistics enabled by this command, use the **show call application interface** command. To reset the interface counters to zero, use the **clear call application interface** command.

Examples The following example enables statistics collection for application interfaces:

```
application
    monitor
    interface stats
```

Related Commands

Command	Description
call application interface stats	Enables statistics collection for application interfaces.
clear call application interface	Clears application interface statistics or event logs.
interface event-log	Enables event logging for external interfaces used by voice applications.
show call application interface	Displays event logs and statistics for application interfaces.
stats	Enables statistics collection for voice applications.

ip circuit

To create carrier IDs on an IP virtual trunk group, and create a maximum capacity for the IP group, use the **ip circuit** command. To remove a trunk group or maximum capacity, use the **no** form of the command.

ip circuit {**carrier-id** *carrier-name* [**reserved-calls** *reserved*] | **max-calls** *maximum-calls* | **default** {**only** | **name** *carrier-name*}}

no ip circuit {**carrier-id** *carrier-name* | **default** {**only** | **name** *carrier-name*}}

Syntax Description

carrier-id	Sets the IP circuit associated with a specific carrier.
carrier-name	Defines an IP circuit using the specified name as the circuit ID.
reserved-calls *reserved*	(Optional) Specifies the maximum number of calls for the circuit ID. Default value is 200.
max-calls *maximum-calls*	Sets the number of maximum aggregate H.323 IP circuit carrier call legs. Default value is 1000.
default only	Creates a single carrier using the default carrier name.
default name	Changes the default circuit name.
carrier-name	Default carrier name.

Command Default

If this command is not specified, no IP carriers and no maximum call leg values are defined.

Command Modes

H.323 configuration.

Command History

Release	Modification
12.2(13)T3	This command was introduced.

Usage Guidelines

You can use the **ip circuit** command only when no calls are active. You can define multiple carrier IDs, and the ordering does not matter. IP circuit default only is mutually exclusive with defining carriers with circuit carrier id.

If **ip circuit default only** is specified, the maximum calls value is set to 1000.

Examples

The following example specifies a default circuit and maximum number of calls:

```
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
```

The following example specifies a default carrier and incoming source carrier:

```
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
  h323
   ip circuit carrier-id AA reserved-calls 200

   ip circuit max-calls 1000
```

Related Commands

Command	Description
show crm	Displays some of the values set by this command.
voice-source group	Assigns a name to a set of source IP group characteristics, which are used to identify and translate an incoming VoIP call.

ip dhcp-client forcerenew

To enable forcerenew-message handling on the DHCP client when authentication is enabled, use the **ip dhcp-client forcerenew** command in global configuration mode. To disable the forced authentication, use the **no** form of this command.

ip dhcp-client forcerenew

no ip dhcp-client forcerenew

Syntax Description This command has no arguments or keywords.

Command Default Forcerenew messages are dropped.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines DHCP forcerenew handling is not enabled until the CLI is configured.

Examples The following example shows how to enable DHCP forcerenew-message handling on the DHCP client:

```
Router(config)# ip dhcp-client forcerenew
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
key chain	Identifies a group of authentication keys for routing protocols.

ip precedence (dial peer)

To set IP precedence (priority) for packets sent by the dial peer, use the **ip precedence** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

ip precedence *number*

no ip precedence *number*

Syntax Description

number	Integer specifying the IP precedence value. Range is 0 to 7. A value of 0 means that no precedence (priority) has been set. The default is 0.

Command Default The default value for this command is zero (0)

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)NA	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines Use this command to configure the value set in the IP precedence field when voice data packets are sent over the IP network. This command should be used if the IP link utilization is high and the quality of service for voice packets needs to have a higher priority than other IP packets. This command should also be used if RSVP is not enabled and the user would like to give voice packets a higher priority than other IP data traffic.

This command applies to VoIP peers.

Examples The following example sets the IP precedence to 5:

```
dial-peer voice 10 voip
 ip precedence 5
```

ip qos defending-priority

To configure the Resource Reservation Protocol (RSVP) defending priority value for determining quality of service (QoS), use the **ip qos defending-priority** command in dial peer configuration mode. To disable RSVP defending priority as a QoS factor, use the **no** form of this command.

ip qos defending-priority *defending-pri-value*

no ip qos defending-priority

Syntax Description

defending-pri-value	The RSVP defending priority value for determining QoS priorities. Valid entries are from 0 to 65535.

Command Default

The RSVP defending priority value is disabled and is not a factor in determining QoS.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

To configure the RSVP defending priority value, use the **ip qos defending-priority** command in dial peer configuration mode. The defending priority value is passed to the QoS module during reservation initiation. In a situation where there is not enough bandwidth available to support all calls, this setting enables an existing call to avoid being preempted by a new call unless the preemption priority of the new call is higher than the defending priority of the existing call.

Examples

The following example shows how to specify the RSVP defending priority value:

```
dial-peer voice 100 voip
 ip qos defending-priority 1111
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
ip qos dscp	Configures the DSCP value for QoS.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos preemption-priority	Configures the RSVP preemption priority.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.
show-sip-ua calls	Displays the active UAC and UAS information for SIP calls on a Cisco IOS device.
voice-class sip rsvp-fail-policy	Configures RSVP failure policies.

ip qos dscp

To configure the differentiated services code point (DSCP) value for quality of service (QoS), use the **ip qos dscp** command in dial peer configuration mode. To disable DSCP as a QoS factor, set the DSCP value to **default** (which sets the value to the 000000 bit pattern). To set DSCP values to their default settings, use the **no** form of this command.

ip qos dscp {*dscp-value* | *set-af* | *set-cs* | **default** | **ef**} {**signaling** | **media** [**rsvp-pass** | **rsvp-fail**] | **video** [**rsvp-none** | **rsvp-pass** | **rsvp-fail**]}

no ip qos dscp {*dscp-value* | *set-af* | *set-cs* | **default** | **ef**} {**signaling** | **media** [**rsvp-pass** | **rsvp-fail**] | **video** [**rsvp-none** | **rsvp-pass** | **rsvp-fail**]}

Syntax Description

dscp-value	DSCP value. Valid entries are from 0 to 63.
set-af	An assured forwarding bit pattern as the DSCP value: • **af11**—bit pattern 001010 • **af12**—bit pattern 001100 • **af13**—bit pattern 001110 • **af21**—bit pattern 010010 • **af22**—bit pattern 010100 • **af23**—bit pattern 010110 • **af31**—bit pattern 011010 • **af32**—bit pattern 011100 • **af33**—bit pattern 011110 • **af41**—bit pattern 100010 • **af42**—bit pattern 100100 • **af43**—bit pattern 100110
set-cs	Class-selector code point as the DSCP value: • **cs1**—code point 1 (precedence 1) • **cs2**—code point 2 (precedence 2) • **cs3**—code point 3 (precedence 3) • **cs4**—code point 4 (precedence 4) • **cs5**—code point 5 (precedence 5) • **cs6**—code point 6 (precedence 6) • **cs7**—code point 7 (precedence 7)
default	Specifies the default bit pattern 000000 as the DSCP value.
ef	Specifies the expedited forwarding bit pattern 101110 as the DSCP value.
signaling	Specifies that the DSCP value applies to signaling packets.
media	Specifies that the DSCP value applies to media packets (voice and fax).
rsvp-pass	(Optional) Specifies that the DSCP value applies to packets with successful Resource Reservation Protocol (RSVP) reservations.
rsvp-fail	(Optional) Specifies that the DSCP value applies to packets (media or video) with failed RSVP reservations.
video	Specifies that the DSCP value applies to video packets. This option is valid only for Cisco Unified Communications Manager Express (Cisco Unified CME) on a Cisco Unified Border Element.
rsvp-none	(Optional) Specifies that the DSCP value applies to video packets with no RSVP reservations (valid only for video packets.)

Command Default

The DSCP default values are as follows**:**

- The default DSCP value for all signaling packets is **af31**.
- The default DSCP value for all media (voice and fax) packets is **ef**.
- The default DSCP value for all video packets is **af41**.

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)T	This command was introduced. It replaced the **ip precedence** (dial peer) command
12.3(4)T	Keywords were added to support DSCP configuration for video streams.
12.4(22)T	Keywords were added to apply a DSCP value to media (voice and fax) packets with a specified (successful or failed) RSVP connection.

Usage Guidelines To configure voice, signaling, and video traffic priorities, use the **ip qos dscp** command in dial peer configuration mode. The recommended value for media (voice and fax) packets is **ef;** for signaling packets, the recommended value is **af31**; and for video packets, it is **af41** (all defaults).

Additionally, before you can specify RSVP QoS, you must first use the **ip rsvp bandwidth** command to enable RSVP on the IP interface.

Examples The following example shows how to set the DSCP value to a class-selector code point value of 1 and apply that DSCP setting to media (voice and fax) payload packets with no RSVP configured:

```
dial-peer voice 1 voip
 ip qos dscp cs1 media
```

The following example shows how to set the DSCP value to the expedited forwarding bit pattern and apply that DSCP setting to media (voice and fax) payload packets with a successful RSVP connection:

```
dial-peer voice 1 voip
ip qos dscp ef media rsvp-pass
```

The following example shows how to set the DSCP value to an assured forwarding code point value of 22 and apply that DSCP setting to all signaling packets:

```
dial-peer voice 1 voip
ip qos dscp af22 signaling
```

The following example shows how to set the DSCP value to an assured forwarding code point value of 43 and apply that DSCP setting to video packets with a successful RSVP connection:

```
dial-peer voice 100 voip
 ip qos dscp af43 video rsvp-pass
```

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP signaling and the voice signaling protocol.
ip qos defending-priority	Configures the RSVP defending priority value.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos preemption-priority	Configures the RSVP preemption priority value.

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp signalling dscp	Configures the DSCP settings to be used on RSVP messages on an interface.

ip qos policy-locator

To configure a quality of service (QoS) policy-locator (application ID) used to deploy Resource Reservation Protocol (RSVP) policies for specifying bandwidth reservations on Cisco IOS Session Initiation Protocol (SIP) devices, use the **ip qos policy-locator** command in dial peer configuration mode. To delete an application policy, use the **no** form of this command.

ip qos policy-locator {**video** | **voice**} [**app** *app-string*] [**guid** *guid-string*] [**sapp** *subapp-string*] [**ver** *version-string*]

no ip qos policy-locator {**video** | **voice**} [**app** *app-string*] [**guid** *guid-string*] [**sapp** *subapp-string*] [**ver** *version-string*]

Syntax Description

video	Specifies that the application ID applies to RSVP for video streams.
voice	Specifies that the application ID applies to RSVP for voice streams.
app	(Optional) Specifies an application.
app-string	Application ID. Consists of 1 to 31 alphanumeric characters.
guid	(Optional) Specifies a globally unique identifier (GUID).
guid-string	GUID. Consists of 1 to 31 alphanumeric characters.
sapp	(Optional) Specifies a subapplication.
sapp-string	Subapplication ID. Consists of 1 to 31 alphanumeric characters.
ver	(Optional) Specifies a version.
ver-string	Version ID. Consists of 1 to 15 alphanumeric characters.

Command Default

No policy is specified.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

In Cisco IOS software, the RSVP can process and accept requests by referring to multiple bandwidth pools. To enhance the granularity of local policy match criteria on Cisco IOS SIP devices, bandwidth pools can include policies based on application IDs. You can use these application-specific IDs to reserve bandwidth for each until specified bandwidth limits are reached.

To prevent one application type from consuming all bandwidth, RFC 2872, *Application and Sub Application Identity Policy Element for Use with RSVP*, allows for the creation of separate bandwidth reservation pools. For example, an RSVP reservation pool can be created for voice traffic and another for video traffic so that reservations tagged with these application IDs can then be matched to the interface bandwidth pools using RSVP local policies. To limit bandwidth per application, though, you must configure a bandwidth limit for each application and configure each with a reservation flag that associates the application with the appropriate bandwidth limit.

Before you can configure bandwidth limits for any application-specific policy, however, you must create application IDs. To create application IDs (application-specific reservation profiles), use the **ip qos policy-locator** command in dial peer configuration mode. After creating the necessary application IDs, you can then use the appropriate commands listed in the "Related Commands" section to configure bandwidth reservation. However, this feature is available only on supported devices that are running Cisco IOS Release 12.4(22)T or a later release.

For more information about configuring SIP RSVP features, see the "Configuring SIP RSVP Features" chapter in the *Cisco IOS SIP Configuration Guide*. For more general information about the application-specific policy feature, see the "Configuring RSVP" chapter in the RSVP section of the "Signaling" part in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example shows how to configure a policy for the application ID:

```
dial-peer voice 100 voip
 ip qos policy-locator voice app MyApp1 sapp MySubApp4
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
handle-replaces	Configures fallback to legacy handling of SIP INVITE.
ip qos defending-priority	Configures the RSVP defending priority value.
ip qos dscp	Sets the DSCP value for QoS.
ip qos preemption-priority	Configures the RSVP preemption priority value.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp policy default-reject	Configures blocking or passing of all messages that do not match any existing RSVP policies.
ip rsvp policy identity	Defines RSVP application IDs used to deploy RSVP policies.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
maximum (local policy)	Configures a local policy that limits RSVP resources.
preempt-priority	Configures RSVP QoS priorities to be inserted into PATH and RESV messages when they are not signaled from an upstream or downstream neighbor or local client application.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.
show sip-ua calls	Displays the active UAC and UAS information on SIP calls.
voice-class sip rsvp-fail-policy	Specifies the action that takes place when RSVP negotiation fails.

ip qos preemption-priority

To configure the Resource Reservation Protocol (RSVP) preemption priority value for determining quality of service (QoS), use the **ip qos preemption-priority** command in dial peer configuration mode. To disable RSVP preemption priority as a QoS factor, use the **no** form of this command.

ip qos preemption-priority *preemption-pri-value*

no ip qos preemption-priority

Syntax Description

preemption-pri-value	The RSVP preemption priority value for determining QoS priorities. Valid entries are from 0 to 65535.

Command Default

The RSVP preemption priority value is disabled and is not a factor in determining QoS.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

To configure an RSVP preemption priority value, use the **ip qos preemption-priority** command in dial peer configuration mode. The preemption priority value is passed to the QoS module during reservation initiation. In a situation where there is not enough bandwidth available to support all calls, this setting enables a new call to preempt an existing call unless the defending priority of the existing call is higher than the preemption priority of the new call.

Examples

The following example shows how to specify the RSVP preemption priority value:

```
dial-peer voice 100 voip
 ip qos preemption-priority 1111
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
ip qos dscp	Configures the DSCP value for QoS.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos defending-priority	Configures the defending priority value of RSVP.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.
show-sip-ua calls	Displays the active UAC and UAS information for SIP calls on a Cisco IOS device.
voice-class sip rsvp-fail-policy	Configures RSVP failure policies.

ip rtcp report interval

To configure the average reporting interval between subsequent Real-Time Control Protocol (RTCP) report transmissions, use the **ip rtcp report interval** command in global configuration mode. To reset to the default, use the **no** form of this command.

ip rtcp report interval *value*

no ip rtcp report interval

Syntax Description

value	Average interval for RTCP report transmissions, in ms. Range is 1 to 65535. Default is 5000.

Command Default

5000 ms

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

This command configures the average interval between successive RTCP report transmissions for a given voice session. For example, if the *value* argument is set to 25,000 milliseconds, an RTCP report is sent every 25 seconds, on average.

For more information about RTCP, see RFC 1889, *RTP: A Transport Protocol for Real-Time Applications.*

Examples

The following example sets the reporting interval to 5000 ms:

```
Router(config)# ip rtcp report interval 5000
```

Related Commands

Command	Description
debug ccsip events	Displays all SIP SPI event tracing and traces the events posted to SIP SPI from all interfaces.
timer receive-rtcp	Enables the RTCP timer and configures a multiplication factor for the RTCP timer interval.

ip rtcp sub-rtcp

To specify sub-Real-Time Control Protocol (RTCP) message types, use the **ip rtcp sub-rtcp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip rtcp sub-rtcp *message-type number*

no ip rtcp sub-rtcp *message-type*

Syntax Description

message-type	Message type. For more information, use the question mark (?) online help function.
number	Message number. The range is from 209 to 255. The default is 209. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

RTP payload type is set to the default value 209.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to specify sub-RTCP message typess:

```
Router# configure terminal
Router(config)# ip rtcp sub-rtcp message-type 210
```

Related Commands

Command	Description
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.

ip udp checksum

To calculate the UDP checksum for voice packets sent by the dial peer, use the **ip udp checksum** command in dial peer configuration mode. To disable this feature, use the **no** form of this command.

ip udp checksum

no ip udp checksum

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines Use this command to enable UDP checksum calculation for each of the outbound voice packets. This command is disabled by default to speed up the transmission of the voice packets. If you suspect that the connection has a high error rate, you should enable this command to prevent corrupted voice packets forwarded to the digital signal processor (DSP).

This command applies to VoIP peers.

Note To maintain performance and scalability of the Cisco 5850 when using images before 12.3(4)T, enable no more than 10% of active calls with UDP checksum.

Examples The following example calculates the UDP checksum for voice packets sent by dial peer 10:

```
dial-peer voice 10 voip
 ip udp checksum
```

Related Commands

Command	Description
loop-detect	Enables loop detection for T1 for Voice over ATM, Voice over Frame Relay, and Voice over HDLC.

irq global-request

To configure the gatekeeper to send information-request (IRQ) messages with the call-reference value (CRV) set to zero, use the **irq global-request** command in gatekeeper configuration mode. To disable the gatekeeper from sending IRQ messages, use the **no** form of this command.

irq global-request

no irq global-request

Syntax Description This command has no arguments or keywords.

Command Default The gatekeeper sends IRQ messages with the CRV set to zero.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines Use this command to disable the gatekeeper from sending an IRQ message with the CRV set to zero when the gatekeeper requests the status of all calls after its initialization. Disabling IRQ messages can eliminate unnecessary information request response (IRR) messages if the reconstruction of call structures can be postponed until the next IRR or if the call information is no longer required because calls are terminated before the periodic IRR message is sent. Disabling IRQ messages is advantageous if direct bandwidth control is not used in the gatekeeper.

Examples The following example shows that IRQ messages are not sent from the gatekeeper:

```
.
.
.
 lrq reject-resource-low
 no irq global-request
 timer lrq seq delay 10
 timer lrq window 6
 timer irr period 6
 no shutdown
.
.
.
```

Related Commands

Command	Description
timer irr period	Configures the IRR timer.

isdn bind-l3

To configure an ISDN D-channel serial interface for signaling backhaul and associate it with a session set, use the **isdn bind-l3** command in interface configuration mode. To disable signaling backhaul on an ISDN D-channel serial interface, use the **no** form of this command.

isdn bind-l3 *set-name*

no isdn bind-l3

Syntax Description

set-name	Session set with which you are associating a D-channel interface.

Command Default

The ISDN D channel is not configured for signaling backhaul and is not associated with a session set

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associate the D channel with the session set named “Set1”:

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-L3 set1
Router(config-if)# exit
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named “Set3”:

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-L3 set3
Router(config-if)# exit
```

isdn bind-l3 (Interface BRI)

To cause a Basic Rate Interface (BRI) port to bind ISDN Layer 3 protocol to either a regular gateway (GW) q931 stack or a Cisco CallManager Transmission Control Protocol (TCP) backhaul application and, if the latter, to operate in Media Gateway Control Protocol (MGCP) mode for backhaul, use the **isdn bind-l3** command in interface-BRI configuration mode. To disable binding and reset the BRI to Session Application mode for backhaul, use the **no** form of this command.

isdn bind-l3 {**q931** | **ccm-manager service mgcp**}

no isdn bind-l3 {**q931** | **ccm-manager service mgcp**}

Syntax Description

q931	Regular GW q931 stack. This is the default.
ccm-manager service mgcp	Cisco CallManager TCP backhaul application. You must also select MGCP service mode for backhaul.

Command Default

If the command is not used, the BRI port uses Session Application mode and binding is disabled. If the command is used with no keywords, q931 is assumed.

Command Modes

Interface-BRI configuration

Command History

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

This command reinitializes the BRI interface, including the two B-channel voice ports within the BRI, to support MGCP-backhaul call control. It also binds ISDN Q931 Layer 3 to the Cisco CallManager.

This command is visible when the BRI voice interface card (VIC) is present. The BRI VIC provides narrowband digital-voice connectivity in the voice network module on the Cisco 2600 series and Cisco 3600 series.

Before you use this command to enable binding, disable any active calls on the BRI interface by using the **shutdown** (voice-port) command. You need not shut down the interface if no active calls are present or to configure L3 binding.

The combined **ccm-manager service mgcp** keywords are available only for supported BRI interfaces.

Examples

The following example sets binding for BRI interface slot 1, port 0:

```
Router (config-if)# isdn bind-l3 q931
```

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers, their current status, and their availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp	Displays values for MGCP parameters.
shutdown (voice-port)	Takes voice ports for a specific VIC offline.

isdn bind-l3 ccm-manager

To bind Layer 3 of the ISDN PRI interface of the Media Gateway Control Protocol (MGCP) voice gateway to the Cisco CallManager for PRI Q.931 signaling backhaul support, use the **isdn bind-l3 ccm-manager** command in interface configuration mode. To disable this binding, use the **no** form of this command.

isdn bind-l3 ccm-manager

no isdn bind-l3 ccm-manager

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Interface configuration

Command History

Release	Modification
12.2(2)XN	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2, and implemented on the Cisco IAD2420.

Usage Guidelines This command enables ISDN PRI backhaul on an MGCP-enabled voice gateway.

Examples The following example binds PRI Layer 3 to the Cisco CallManager:

```
isdn bind-l3 ccm-manager
```

isdn bind-l3 iua-backhaul

To specify ISDN backhaul using Stream Control Transmission Protocol (SCTP) for an interface and to bind Layer 3 to DUA for DPNSS backhaul, use the **isdn bind-l3 iua-backhaul** command in interface configuration mode. To disable the backhaul capability, use the **no** form of this command.

isdn bind-l3 iua-backhaul [*application-server-name*]

no isdn bind-l3 iua-backhaul

Syntax Description

application-server-name	(Optional) Name of the application server (AS) to use for backhauling the interface.

Command Default No default behavior or values

Command Modes Interface configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco IAD2420 series. The Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(15)ZJ	The capability to bind Layer 3 to DUA for DPNSS backhaul was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines DPNSS is not configured for backhaul and is not associated with a session set.

Examples The following example configures DUA for DPNSS backhaul using an AS called “as1:”

```
Router(config-if)# isdn bind-l3 iua-backhaul as1
```

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associates the D channel with the session set named “set1”:

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-l3 set1
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named “set3”:

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-l3 set3
```

The following example shows IUA backhaul on the application server “as1”:

```
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-L3 iua-backhaul as1
```

Related Commands

Command	Description
as	Defines an AS for backhaul.
asp	Defines an ASP for backhaul.

isdn contiguous-bchan

To configure contiguous bearer channel handling on an E1 PRI interface, use the **isdn contiguous-bchan** command in interface configuration mode. To disable the contiguous B-channel handling, use the **no** form of this command.

isdn contiguous-bchan

no isdn contiguous-bchan

Syntax Description This command has no arguments or keywords.

Command Default Contiguous B channel handling is disabled

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use this command to specify contiguous bearer channel handling so that B channels 1 to 30, skipping 16, map to time slots 1 to 31. This is available for E1 PRI interfaces only, when the **primary-qsig** or **primary-dms100** switch type option is configured by using the **isdn switch-type** command.

Examples The following example shows the configuration on the E1 interface of a Cisco 3660 router E1 interface:

```
interface Serial5/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn continuous-bchan
```

Related Commands

Command	Description
isdn switch-type	Configures the **primary-qsig** or **primary-dms100** switch type for PRI support.

isdn dpnss

To indicate whether ISDN DPNSS is to act as PBX A or PBX B, or revert to Layer 2, use the **isdn dpnss** command in interface configuration mode. To reset to the default, use the **no** form of this command.

isdn dpnss [**pbxA | layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]

no isdn dpnss [**pbxA | layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]

Syntax Description

pbxA	(Optional) Enables DPNSS to act as PBX A.
layer 2	(Optional) Reverts to Layer 2.
retry max-count *range*	(Optional) Selects the number of times a frame will be retried if unacknowledged. The max-count value can be any number from 0 to 64. Default is 4
timers	(Optional) Selects DPNSS timers, which can be **Tretry** or **Ttest**.
Tretry *timer-value*	(Optional) Sets the Tretry timer in ms and seconds. Valid retry time values range from 5 ms to 10 seconds. Default is 500 ms.
Ttest *timer-value*	(Optional) Sets the Ttest timer in minutes. When the Ttest timer expires, frames are sent on all the DLCs. Valid test time values range from 1 to 60. Default is 5.
test frame	(Optional) Allows test frames to be sent periodically.

Command Default

PBX B

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example sets ISDN DPNSS to act as PBX A:

```
Router(config-if)# isdn dpnss pbxA
```

The following example sets the Tretry and Ttest timers:

```
Router(config-if)# isdn dpnss layer2 timers Tretry 500 Ttest 5
```

The following example selects the number of times a frame will be retried if unacknowledged:

```
Router(config-if)# isdn dpnss layer2 retry max-count 4
```

The following example allows test frames to be sent periodically:

```
Router(config-if)# isdn dpnss layer2 test frame
```

Related Commands

Command	Description
isdn bind-l3 iua-backhaul	Binds Layer 3 for DPNSS to DUA.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN interface.

isdn gateway-max-interworking

To prevent an H.323 gateway from checking for ISDN protocol compatibility and dropping information elements (IEs) in call messages, use the **isdn gateway-max-interworking** command global configuration mode. To reset to the default, use the **no** form of this command.

isdn gateway-max-interworking

no isdn gateway-max-interworking

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway checks for protocol compatibility.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If this command is enabled on an originating H.323 gateway, the information elements (IEs) in call messages to the terminating gateway are not checked for end-to-end protocol compatibility. If this command is enabled on a terminating gateway, IEs are not checked in the reverse direction. If this command is not enabled, and the ISDN protocols are not compatible on the originating and terminating gateways, the gateway drops all IEs, including the progress indicator. The gateway then inserts a progress indicator of 1 into all Progress messages.

Examples

The following example enables maximum interworking:

```
isdn gateway-max-interworking
```

isdn global-disconnect

To allow passage of RELEASE and RELEASE COMPLETE messages over a voice network, use the **isdn global-disconnect** command in interface configuration mode. To disallow passage of RELEASE and RELEASE COMPLETE messages, use the **no** form of this command.

isdn global-disconnect

no isdn global-disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

RELEASE and RELEASE COMPLETE messages terminate locally; they are not passed over the voice network.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.4(15)XY	Support was added for SIP voice networks.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **isdn global-disconnect** command works with ISDN interfaces configured for Q-signaling (QSIG) tunneling using the bri-qsig or pri-qsig ISDN switch type (in either master or slave mode). This command must be enabled on both IP to time-division multiplexing (IP-TDM) gateways in a toll-bypass scenario where RELEASE and RELEASE COMPLETE messages need to be transparently passed end-to-end and in both directions.

Enabling the **isdn global-disconnect** command allows passage of the RELEASE and RELEASE COMPLETE messages (including information element (IE) content) end-to-end across a voice network between PBXs. Use the **no** form of this command to prevent RELEASE and RELEASE COMPLETE messages from being passed across the network.

Examples

The following example shows the configuration on the T1 PRI interface of a Cisco 3660 router:

```
interface Serial5/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn global-disconnect
 isdn overlap-receiving
 isdn incoming-voice voice
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the interface to serve as either the QSIG slave or the QSIG master (must be the opposite setting as that set on the PBX.)
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
signaling forward	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages globally for a SIP or H.323 gateway.
signaling forward (dial-peer)	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages for a specific dial peer on a SIP or H.323 gateway.

isdn gtd

To enable generic transparency descriptor (GTD) mapping for information elements (IEs) sent in ISDN Setup messages, use the **isdn gtd** command in interface configuration mode. To disable GTD mapping, use the **no** form of this command.

isdn gtd

no isdn gtd

Syntax Description This command has no arguments or keywords.

Command Default GTD mapping is enabled.

Command Modes Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines Use the **isdn gtd** command to enable parameter mapping for the following ISDN IEs to corresponding GTD parameters:

- Originating Line Information—OLI
- Bearer Capability—USI and TMR
- Called Party Number—CPN
- Calling Party Number—CGN
- Redirecting Number—RGN, OCN and RNI

The following GTD parameters, which have no corresponding ISDN IEs, are also supported:

- Calling Party Category—CPC
- Forward Call Indicators—FCI
- Protocol Name—PRN

Examples The following example enables GTD parameter mapping:

```
isdn gtd
```

isdn ie oli

To configure the value of the Originating Line Information (OLI) information element (IE) identifier when the gateway receives ISDN signaling from an MCI switch, use the **isdn ie oli** command in interface configuration mode. To disable the OLI IE identifier, use the **no** form of this command.

isdn ie oli *value*

no isdn ie oli *value*

Syntax Description

value	Hexadecimal number specifying the value that indicates OLI information from the MCI switch. Range is 00-7F.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **isdn ie oli** command to configure gateway support for the MCI ISDN variant by specifying the IE value that indicates OLI information.

Examples

The following example configures the OLI IE value to a hex value of 7A:

```
isdn ie oli 7A
```

Related Commands

Command	Description
isdn gtd	Enables GTD parameter mapping for ISDN IEs.

isdn integrate calltype all

To enable integrated mode on an ISDN PRI interface, use the **isdn integrate calltype all** command in interface configuration mode. To disable integrated mode, use the **no** form of this command.

isdn integrate calltype all

no isdn integrate calltype all

Syntax Description This command has no arguments or keywords.

Command Default Integrated mode is disabled on the interface.

Command Modes Interface configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines Configure this command from a PRI interface only. This command is not supported from a BRI interface.

Any incoming calls from an interface that has been configured for integrate calltype all is rejected with cause-code **invalid number 0x1C** if inbound dial-peer is not selected.

Examples In the following example, the interface is shut down.

```
Router(config)# interface Serial4/1:15
Router(config-if)# shutdown
```

In the following example, integrated mode is enabled.

```
Router(config)# interface Serial4/1:15
Router(config-if)# isdn integrate calltype all
% This command line will enable the Serial Interface to "integrated service" mode.
% The "isdn incoming-voice voice" setting will be removed from the interface.
% Continue? [confirm]
```

When you confirm, the default incoming-voice configuration is removed from the interface, and the interface is now in integrated service mode. The interface does not reset back to voice mode if an incoming call is originated from the interface.

In the following example, the interface is set to active.

```
Router(config)# interface Serial4/1:15
Router(config-if)# no shutdown
```

Related Commands

Command	Description
dial-peer data	Creates a data dial peer and enters dial peer configuration mode.
dial-peer search	Optimizes voice or data dial-peer searches.
isdn incoming-voice	Routes all incoming voice calls to the modem and determine how they will be treated.

isdn network-failure-cause

To specify the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures, use the **isdn network-failure-cause** command in interface configuration mode. To disable use of this cause code, use the **no** form of this command.

isdn network-failure-cause *value*

no isdn network-failure-cause *value*

Syntax Description

value	Number, from 1 to 127. See Table 31 for a list of failure cause code values.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

The PBX can reroute calls based on the cause code returned by the router.

This command allows the original cause code to be changed to the value specified if the original cause code is not one of the following:

- NORMAL_CLEARING (16)
- USER_BUSY (17)
- NO_USER_RESPONDING (18)
- NO_USER_ANSWER (19)
- NUMBER_CHANGED (22)
- INVALID_NUMBER_FORMAT (28)
- UNSPECIFIED_CAUSE (31)
- UNASSIGNED_NUMBER (1)

Table 31 describes the cause codes.

Table 31 ISDN Failure Cause Codes

Failure Cause Code	Meaning
1	Unallocated or unassigned number.
2	No route to specified transit network.
3	No route to destination.

Table 31 ISDN Failure Cause Codes (continued)

Failure Cause Code	Meaning
6	Channel unacceptable.
7	Call awarded and being delivered in an established channel.
16	Normal call clearing.
17	User busy.
18	No user responding.
19	No answer from user (user alerted).
21	Call rejected.
22	Number changed.
26	Nonselected user clearing.
27	Destination out of order.
28	Invalid number format.
29	Facility rejected.
30	Response to status enquiry.
31	Normal, unspecified.
34	No circuit/channel available.
38	Network out of order.
41	Temporary failure.
42	Switch congestion.
43	Access information discarded.
44	Requested channel not available.
45	Preempted.
47	Resources unavailable, unspecified.
49	Quality of service unavailable.
50	Requested facility not subscribed.
52	Outgoing calls barred.
54	Incoming calls barred.
57	Bearer capability not authorized.
58	Bearer capability not available now.
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital information bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference value.
82	Identified channel does not exist.

Table 31 ISDN Failure Cause Codes (continued)

Failure Cause Code	Meaning
83	Suspended call exists, but this call ID does not.
84	Call ID in use.
85	No call suspended.
86	Call with requested call ID is cleared.
88	Incompatible destination.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type nonexistent or not implemented.
98	Message not compatible with call state or message type nonexistent or not implemented.
99	Information element nonexistent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state.
102	Recovery on timer expiry.
111	Protocol error, unspecified.
127	Interworking, unspecified.

Examples

The following example specifies a cause code to pass to a PBX when a call cannot be placed or completed of internal network failures:

```
isdn network-failure-cause 28
```

isdn outgoing display-ie

To enable the display information element to be sent in the outgoing ISDN message if provided by the upper layers, such as voice or modem. To disable the displaying of the information element in the outgoing ISDN message, use the no form of this command.

isdn outgoing display-ie

no isdn outgoing display-ie

Syntax Description There are no arguments or keywords.

Command Default No default behavior or values

Command Modes Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines The **isdn outoing display-ie** command is direction dependent, such as network-to-user or user-to-network. Not all ISDN switch types support the **isdn outgoing display-ie** command. The following shows the direction dependency by switch type, and this command can be used to override the dependency:

- ETSI (NTT, NET3,and NET5)—Only network-to-user
- DMS—Both ways
- TS014—Only network-to-user
- TS013—Only network-to-user
- 1TR6—Only network-to-user

Note The 4ESS, 5ESS, NI1, and NI2 switch types are not supported in any direction.

Note When the **isdn protocol-emulate** command is switched between network and user, this command reverts to its default value. The **isdn outoing display-ie** command must be enabled again.

Examples

The following is a running configuration, showing how the the **isdn outgoing display-ie** command is used on a specified serial interface:

```
Router# show running-config interface serial0:23
interface Serial0:23
 no ip address
 dialer idle-timeout 999999
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn T310 30000
 isdn outgoing display-ie
```

Related Commands

Command	Description
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn protocol-emulate

To emulate the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type, use the **isdn protocol-emulate** command in interface configuration mode. To disable ISDN emulation, use the **no** form of this command.

isdn protocol-emulate {**network** | **user**}

no isdn protocol-emulate {**network** | **user**}

Syntax Description

network	Network side of an ISDN configuration.
user	User side of an ISDN configuration.

Command Default No default behavior or values

Command Modes Interface configuration mode

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 concentrator.
12.1(1)T	This command was introduced in the T train.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. This command is not supported on the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3	This command was enhanced to support network emulation capability on the Lucent 4ESS, 5ESS, and Nortel DMS-100 ISDN switch types. These switch types can be configured as a network, but no additional changes were made and not all network side features are supported.
12.3(8)T	Added support for the PRI NTT switch type.

Usage Guidelines

- The current ISDN signaling stack can emulate the ISDN network side, but it does not conform to the specifications of the various switch types in emulating the network side.
- This command enables the Cisco IOS software to replicate the public switched network interface to a Private Branch Exchange (PBX).
- To emulate NT (network) or TE (user) functionality, use this command to configure the layer 2 and layer 3 port protocol of a BRI voice port or a PRI interface.

- Use this command to configure the Cisco AS5300 PRI interface to serve as either the primary QSIG slave or the primary QSIG master. To disable QSIG signaling, use the **no** form of this command; the layer 2 and layer 3 protocol emulation defaults to **user**.
- This feature is supported for the PRI Net5 and PRI NTT switch types.

Examples

The following example configures the interface (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# int s0:15
Router(config-if)# isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of T1 PRI interface 23 to act as the QSIG master (NT):

```
interface serial 1:23
 isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of a BRI voice port to operate as QSIG slave (TE):

```
interface bri 1
 isdn protocol-emulate user
```

The following example configures the layer 2 and layer 3 function of an E1 PRI interface to operate as QSIG slave (TE):

```
interface serial 4:23
 isdn protocol-emulate user
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make outgoing call selection in ascending, descending, or round-robin order.
isdn logging	Enables logging of ISDN syslog messages.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn rlm-group

To specify a Redundant Link Manager (RLM) group number for ISDN to use, enter the **isdn rlm-group** command in controller configuration mode. To disable this function, use the **no** form of this command.

isdn rlm-group *number*

no isdn rlm-group *number*

Syntax Description

number	Number of the RLM group. Valid range is from 0 to 5.

Command Default

No RLM group is specified and the ISDN D channel is reserved for signaling information.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.4(16)	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(15)T	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

RLM delivers ISDN Q.921 frames over an IP network. RLM affects D-channel signaling only; it does not affect the B channels. The time slot assigned originally to the D channel is freed and used as a B channel because D signaling occurs over the IP network.

The **isdn rlm-group** command allows RLM to be used to transport the D-channel information (signaling) over Ethernet.

The **isdn rlm-group** is supported only on the Cisco AS5300, AS5350, AS5400, and AS5850 series access servers. This command is not supported on Cisco 1800 series, 2800 series, 3700 series, and 3800 series platforms.

Prior to Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command could be entered on Cisco 2800 series and 3800 series platforms even though it was not supported. In some conditions, this could cause the router to reload. Effective with Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command is no longer available on the Cisco 2800 series and 3800 series platforms.

Examples

The following example defines RLM group 1:

```
interface Serial0:23
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 dialer map ip 10.0.0.2 name map1 1111111
```

```
dialer load-threshold 1 either
dialer-group 1
isdn switch-type primary-ni
isdn incoming-voice modem
isdn rlm-group 1
ppp authentication chap
ppp multilink
hold-queue 75 in
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a specified amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

isdn skipsend-idverify

To stop the user side of a BRI interface from sending ID verify information, use the **isdn skipsend-idverify** command in interface configuration mode. To restore the user-side notification, use the **no** form of this command.

isdn skipsend-idverify

no isdn skipsend-idverify

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the user side sends the ID verify information. The **no** form of this command is in effect by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

For user-side BRI interfaces, you can send ID verify messages to confirm the status of a particular terminal endpoint identifier (TEI) when there is doubt about whether the TEI is in use (for example, after a Layer 1/Layer 2 flap). ID is the TEI value.

For network-side BRI interfaces, the command should always be set. In some cases, the command will automatically be configured after the BRI network-side protocol emulation is set. If not, you can manually configure the command on the network-side BRI interface. After the command has been configured either automatically or manually, it cannot be further changed. A network-side BRI interface should always be set so that it does not send ID verify information.

Examples

The following example shows user-side output, with the default in effect, so the ID verify is sent:

```
Router# show isdn status br0/0

Global ISDN Switchtype = basic-net3
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 95, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

The following sample output shows network-side output, with the default in effect:

```
ISDN BRI1/1 interface
        ******* Network side configuration *******
        dsl 9, interface ISDN Switchtype = basic-qsig
         **** Master side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 9 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

The following sample output shows the BRI interface with the **isdn skipsend-idverify** command in effect (so the ID verify will *not* be sent):

```
Router# show run interface br0/0

Building configuration...

Current configuration : 185 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
 isdn skipsend-idverify
end
```

The following example shows the return to default so that the ID verify will be sent:

```
Router# configure

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface br0/0
Router(config-if)#no isdn skipsend-idverify
Router(config-if)#
```

The following output shows that the skip send has been removed (so the ID verify information *will* be sent):

```
Router# show run interface br0/0

Building configuration...

Current configuration : 161 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
end
```

This configuration example shows the warning message that appears when the command is applied or when the **no** form of the command is entered on a network-side BRI interface:

```
Router# configure

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int br1/1
Router(config-if)#isdn skipsend-idverify
% Network side should never send ID VERIFY <---- warning message
Router(config-if)#
```

Related Commands

Command	Description
interface bri	Specifies the interface and enters interface configuration mode.

isdn spoofing

To enable ISDN spoofing so that loss of Layer 1 or Layer 2 connectivity of the ISDN BRI interface is not detected by the Trunk Group Resource Manager (TGRM) or similar application, use the **isdn spoofing** command in interface configuration mode. To disable ISDN spoofing so the TGRM or similar application can detect when the BRI interface is not operational (when the Layer 1 or Layer 2 connection is down), use the **no** form of this command.

isdn spoofing

no isdn spoofing

Syntax Description

This command has no arguments or keywords.

Command Default

The ISDN BRI interface is spoofing, which means that applications always see the BRI interface connection as operational (unless the interface has been manually shut down [ADMINDOWN state]).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The ISDN BRI interface is spoofing by default. Spoofing makes the ISDN BRI interface available (up) for operation (for dialing in ISDN), even if the interface is down. For an ISDN BRI interface to be set to a down condition, the interface must be manually shut down (IDBS_ADMINDOWN state). Spoofing enables upper layers to dial out even when the interface is down.

Some upper layer modules, such as TGRM and similar applications, allow dial-out only if the channel is available. If the record for TGRM or similar application is notified of the actual status of BRI, then the TGRM or similar application can dial out accordingly. In this case, the **no isdn spoofing** command is appropriate.

Note ISDN spoofing can be applied only to BRI interfaces—it does not apply to PRI interfaces.

Examples

The following example shows how to configure an ISDN BRI interface to disable ISDN spoofing:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface bri0/0
Router(config-if)# no isdn spoofing
Router(config-if)#
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
show isdn status	Displays the status of all ISDN interfaces or a specific ISDN interface.

isdn supp-service calldiversion

To ensure that all calls on an ISDN serial interface can be traced if diverted, use the **isdn supp-service calldiversion** command in interface configuration mode. To disable tracing of diverted ISDN calls, use the **no** form of this command.

isdn supp-service calldiversion

no isdn supp-service calldiversion

Syntax Description

This command has no arguments or keywords.

Command Default

VoIP calls, when diverted, are not traceable and are translated into a Redirection Information Element (RedirectionIE).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

To enable traceability, the call diversion service requires that a VoIP call (when diverted) translates into a divertingLegInformation2 IE instead of a RedirectionIE. When the **isdn supp-service calldiversion** command is configured, the redirecting information coming from the application is packed in the Facility Information Element (FAC IE) as DiversionLeg2 information and sent in the outgoing SETUP message.

The **isdn supp-service calldiversion** command works only for NET5 switches.

Examples

The following example shows how to configure the primary NET5 switch so that the call diversion tracing service is enabled:

```
interface serial3:23
 no ip address
 isdn switch-type primary-net5
 isdn supp-service calldiversion
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, CAS, or robbed-bit signaling.

isdn supp-service mcid

To enable an ISDN serial interface for Malicious Caller Identification (MCID), use the **isdn supp-service mcid** command in interface configuration mode. To disable MCID functionality, use the **no** form of this command.

isdn supp-service mcid

no isdn supp-service mcid

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command. This command is valid only at the ISDN interface level.

Examples

The following configuration example shows MCID enabled for the PRI:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0. 255.255.255.0
 isdn supp-service mcid
 isdn T-Activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary slave (user) or the primary master (network).
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn t-activate	Specifies how long the ISDN serial interface must wait for the malicious caller to be identified.

isdn supp-service name calling

To set the calling name display parameters sent out on an ISDN serial interface, use the **isdn supp-service name calling** command in interface configuration mode. To disable calling name delivery, use the **no** form of this command.

isdn supp-service name calling [**ie** | **operation-value-tag** | **profile** {**Network Extension operation-value-tag** {**ecma** | **iso** | **local**} | **ROSE**}]

no isdn supp-service name calling

Syntax Description

ie	(Optional) Specifies that the value of the calling name information element (ie) is to be sent.
operation-value-tag	(Optional) Specifies that the operation value tag for the calling name is to be sent.
profile	(Optional) Specifies that a particular protocol profile is to be sent.
Network-Extension	Specifies the networking extension (0x9F).
ecma	Specifies that the European Computer Manufacturers' Association (ECMA) object identifier (OID) global value (protocol profile 0x06 04 2B 0C 09 00) is to be sent.
iso	Specifies that the International Standards Organization (ISO) OID global value (protocol profile 0x06 05 28 EC 2C 00 00) is to be sent.
local	Specifies that the local OID global value (protocol profile 0x02 01 00) is to be sent.
ROSE	(Optional) Specifies that the Remote Operations Service Element (ROSE) value (protocol profile 0x91) is to be sent.

Command Default

Calling name delivery is disabled, so no calling-name display parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(15)T1	The **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywordswere added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

Under the serial interface (interface serial command), the **isdn supp-service name calling** command must be configured so that when the calling name comes in the Facility Information Element (IE) of the ISDN setup message, the gateway sends the calling name to the Cisco Unified Communications Manager

as a Display IE. If the **isdn supp-service name calling** command is not configured under the ISDN serial interface, the calling name in the FacilityIE is sent as user-to-user data to the Cisco Unified Communications Manager without the display data.

Beginning with Cisco IOS Release 12.4(15)T1, the **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywords were added to provide more specific information in defining calling name information that is to be sent.

Examples

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice service level:

```
voice service voip
 h323
 h225 display-ie ccm-compatible
```

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice class level:

```
voice class h323 1
 h225 display-ie ccm-compatible [system]
```

The following example shows the H.323 name display information on ISDN trunks:

```
interface Serial0/3/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn map address *. plan isdn type unknown
 isdn supp-service name calling
 isdn bind-l3 ccm-manager
 no cdp enable
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.

isdn supp-service tbct

To enable ISDN Two B-Channel Transfer (TBCT) on PRI trunks, use the **isdn supp-service tbct** command in interface or trunk group configuration mode. To reset to the default, use the **no** form of this command.

isdn supp-service tbct [**notify-on-clear** | **tbct-with-crflg**]

no isdn supp-service tbct

Syntax Description

notify-on-clear	(Optional) ISDN switch notifies the gateway whenever a transferred call is cleared.
tbct-with-crflg	(Optional) Includes the call reference flag while sending a TBCT request.

Command Default

TBCT is disabled.

Command Modes

Interface configuration
Trunk-group configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command enables TBCT for a specific PRI when used in interface configuration mode. This command configures TBCT for all PRIs in a trunk group when used in trunk-group configuration mode.

The **notify-on-clear** keyword is necessary for the gateway to track billing. This keyword is supported only for user-side ISDN interfaces. You must configure the ISDN switch to send a notify message when a call is cleared.

On some PBX switches, the call reference flag (including the call reference value of the other call) is mandatory. To include the call reference flag in a TBCT request, use the **tbct-with-crflg** keyword. The call reference flag can be 00 or 80. So, for example, if the call reference value is 02, the call reference flag is 0002 or 8002.

Examples

The following example shows how to enable TBCT for interface 0:23:

```
interface Serial0:23
 isdn supp-service tbct
```

The following example shows how to enable TBCT for trunk group 1:

```
trunk group 1
 isdn supp-service tbct
```

The following example shows how to include the call reference flag in TBCT requests for trunk group 1:

```
trunk group 1
 isdn supp-service tbct tbct-with-crflg
```

Related Commands

Command	Description
call application voice transfer mode	Specifies the call-transfer behavior of a TCL or VoiceXML application.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max call-duration	Sets the maximum duration allowed for a call that is redirected using TBCT.
tbct max calls	Sets the maximum number of active calls that can use TBCT.
trunk group	Enters trunk-group configuration mode to define or modify a trunk group.

isdn t-activate

To specify how long the gateway waits for a response from the PSTN after sending a MCID request, use the **isdn t-activate** command in interface configuration mode. To disable the timer, use the **no** form of this command.

isdn t-activate *ms*

no isdn t-activate *ms*

Syntax Description

ms	Number of milliseconds (ms). Range is 1000 to 15000. Default is 4000; 5000 is recommended.

Command Default 4000 ms

Command Modes Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines This command starts a timer when the voice gateway sends a Facility message to the PSTN. If a response is not received within the specified time, the TCL IVR script for MCID is notified. Depending on how the script is written, it could reinvoke MCID or perform some other action, such as playing a message if the MCID attempt fails. This command is valid only at the ISDN interface level. The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command.

Examples The following example shows the configuration of the timer on serial interface 0:23:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0 255.255.255.0
 isdn suppserv mcid
 isdn T-Activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary slave (user) or the primary master (network).

Command	Description
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn suppserv mcid	Configures an ISDN serial interface for MCID.

isdn tei-negotiation (interface)

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** command in interface configuration mode. To remove TEI negotiation from an interface, use the **no** form of this command.

isdn tei-negotiation {**first-call** | **powerup**} {**preserve** | **remove**}

no isdn tei-negotiation {**first-call** | **powerup**} {**preserve** | **remove**}

Syntax Description

first-call	ISDN TEI negotiation should occur when the first ISDN call is placed or received.
powerup	ISDN TEI negotiation should occur when the router is powered on.
preserve	Preserves dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shut** and **no shut** EXEC commands are executed.
remove	Removes dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shut** and **no shut** EXEC commands are executed.

Command Default

The **powerup** state is the default condition. Depending upon the ISDN switch type configured, the default will be to preserve or remove the TEI negotiation options. See the "Usage Guidelines" and "Examples" sections for further explanation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3 T	This command was introduced as an interface command.
12.2	The **preserve** and **remove** keywords were added.

Usage Guidelines

This command is for BRI configuration only.

The **first-call** and **powerup**, and **preserve** and **remove** command pairs are mutually exclusive, that is, you must choose only one command from either the **first-call** and **powerup** or **preserve** and **remove** command pairs, per command line.

The **no isdn tei-negotiation** command returns the configuration to default to the **powerup** state.

The **preserve** keyword depends on the ISDN switch type configured, that is, the TEI negotiation configured will be preserved during ISN Layer 1 flaps, and when the **clear interface** or the **shut** and **no shut** EXEC commands are executed, on the switch types listed in Table 32.

Table 32 Switch Types with Preserved TEI Negotiation

Switch Type	Cisco IOS Keyword
French ISDN switch types	**vn2, vn3**
Lucent (AT&T) basic rate 5ESS switch	**basic-5ess**

Table 32 Switch Types with Preserved TEI Negotiation (continued)

Switch Type	Cisco IOS Keyword
Northern Telecom DMS-100 basic rate switch	**basic-dms100**
National ISDN basic rate switch	**basic-ni**
PINX (PBX) switches with QSIG signaling per Q.931	**basic-qsig**

For all other ISDN switch types, the TEI negotiation will be removed during ISDN Layer 1 flaps, and when the **clear interface** or the **shut** and **no shut** EXEC commands are executed. Use the **remove** keyword to specifically set one of the switches listed in Table 32 to the remove state.

Examples

The following example shows the ISDN TEI negotiation configuration with default settings. (Defaults settings do not appear in the router configuration.)

```
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to set TEI negotiation timing to the first call:

```
Router(config-if)# isdn tei-negotiation first-call
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0interface BRI0/0
```

The following example shows how to change TEI negotiation timing back to the default power-up state:

```
Router(config-if)# no isdn tei-negotiation first-call
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to remove TEI negotiation when ISDN Layer 1 flaps (the preserve state is the default for the National ISDN basic rate switch):

```
Router(config-if)# isdn tei-negotiation remove
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 isdn tei-negotiation remove
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to return the National ISDN basic rate switch to its default preserve state:

```
Router(config-if)# no isdn tei-negotiation remove
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

iua

To specify backhaul using Stream Control Transmission Protocol (SCTP) and to enter IDSN User Adaptation Layer (IUA) configuration mode, use the **iua** command in terminal configuration mode.

iua

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines You must first enter IUA configuration mode to access SCTP configuration mode. First enter IUA configuration mode by using the example below and then enter **sctp** at the Router(config-iua)#prompt to bring up SCTP configuration mode. See the **sctp** command.

Examples The following example shows how to enter iua configuration mode:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# iua
Router(config-iua)#
```

The following example shows how to configure the failover-timer by setting the failover time (in milliseconds) to 1 second for a particular AS:

```
Router(config-iua)# as as5400-3 fail-over-timer 1000
```

The following example configure the number of SCTP streams for this AS to 57, which is the maximum value allowed:

```
Router(config-iua)# as as5400-3 sctp-streams 57
```

Related Commands

Command	Description
isdn bind-L3 iua-backhaul	Specifies ISDN backhaul using SCTP for an interface.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

ivr asr-server

To specify the location of an external media server that provides automatic speech recognition (ASR) functionality to voice applications, use the **ivr asr-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr asr-server *url*

no ivr asr-server

Syntax Description

url	Location of the ASR resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr asr-server rtsp://*host***:**[*port*]**/recognizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr asr-server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the *Cisco VoiceXML Programmer's Guide*.

Examples

The following example specifies that voice applications use the ASR server named "asr_serv":

```
Router(config)# ivr asr-server rtsp://asr_serv/recognizer
```

The following example specifies that voice applications use the MRCP v2 ASR server named "asr_mrcpv2serv":

```
Router(config)# ivr asr-server sip:asr_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr tts-server	Specifies the location of a media server that provides TTS functionality to voice applications.
ivr tts-voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr autoload mode

To load files from TFTP to memory using either verbose or silent mode, use the **ivr autoload mode** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload mode {**verbose** [**url** *location*| **retry** *number*]} | {**silent** [**url** *location* | **retry** *number*]}

no ivr autoload mode

Syntax Description

verbose	Displays the file transfer activity to the console. This mode is recommended while debugging.
url *location*	URL that is used to locate the index file that contains a list of all available audio files.
retry *number*	(Optional) Number of times that the system tries to transfer a file when there are errors. This parameter applies to each file transfer. Range is from 1 to 5. Default is 3.
silent	Performs the file transfer in silent mode, meaning that no file transfer activity is displayed to the console.

Command Default Silent

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The index file contains a list of audio files (URL) that can be downloaded from the TFTP server. Use this command to download audio files from TFTP to memory. The command only starts up a background process. The background process (loader) does the actual downloading of the files.

The background process first reads the index file from either Flash or TFTP. It parses the files line by line looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that.au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the mode is set to **verbose**, the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates the background process is not started, and instead you see an error response to the command.

- Check if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts):

  ```
  command is not allowed when prompts are active
  ```

- Check if there is already a background process in progress. If there is a process, the command fails, displaying the following error:

  ```
  previous autoload command is still in progress
  ```

- Check if an earlier **ivr autoload url** command has already been configured. If an **ivr autoload url** command has already been configured, the user sees the following response when the command is issued:

  ```
  previous command is being replaced
  ```

- When the **no ivr autoload url** command is issued, if there was already an **ivr autoload url** command in progress, the original command is aborted.

The audio files (prompts) loaded using the **ivr autoload url** command are not dynamically swapped out of memory. They are considered to be autoloaded prompts, as opposed to dynamic prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)

Examples

The following example configures verbose mode:

```
ivr autoload mode verbose url tftp://blue/orange/tclware/index4 retry 3
```

The following example shows the resulting index file:

```
more index4
tftp://blue/orange/tclware/au/en/en_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash memory:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files occupy in memory.

ivr prompt memory

To configure the maximum amount of memory that the dynamic audio files (prompts) occupy in memory, use the **ivr prompt memory** command in global configuration mode. To disable the maximum memory size, use the **no** form of this command.

ivr prompt memory *size* **files** *number*

no ivr prompt memory

Syntax Description

size	Maximum memory to be used by the free dynamic prompts, in kilobytes. Range is 128 to 16384. The default is 128.
files *number*	Number of files that can stay in memory. Range is 50 to 1000. The default is 200.

Command Default

Memory size: 128 KB
Number of files: 200

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When both the *number* and *size* parameters are specified, the minimum memory out of the two is used for memory calculations.

All the prompts that are not autoloaded or fixed are considered dynamic. Dynamic prompts are loaded in to memory from TFTP or Flash, as and when they are needed. When they are actively used for playing prompts, they are considered to be in “active” state. However, once the prompt playing is complete, these prompts are no longer active and are considered to be in a free state.

The free prompts either stay in memory or are removed from memory depending on the availability of space in memory for these free prompts. This command essentially specifies a maximum memory to be used for these free prompts.

The free prompts are saved in memory and are queued in a wait queue. When the wait queueis full (either because the totally memory occupied by the free prompts exceeds the maximum configured value or the number of files in the wait queue exceeds maximum configured), oldest free prompts are removed from memory.

Examples

The following example sets memory size to 2048 KB and number of files to 500:

```
ivr prompt memory 2048 files 500
```

Related Commands

Command	Description
ivr autoload	Loads files from a particular TFTP server.
show call prompt-mem-usage	Displays the memory site use by prompts.
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr autoload url

To load files from a particular TFTP server (as indicated by a defined URL), use the **ivr autoload** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload url *location*

no ivr autoload url *location*

Syntax Description

url *location*	URL that is to be used to locate the index file that contains a list of all available audio files.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The index file contains a list of audio files URLs that can be downloaded from the TFTP server. Use this command to download audio files from TFTP to memory. The command starts up a background process. The background process (loader) does the actual downloading of the files.

The background process first reads the index file from either Flash memory or TFTP. It parses the files line by line, looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that .au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the *mode* is set to "verbose," in the ivr autoload mode command the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates that the background process is not started, and instead you see an error response to the command.

- Check to see if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts):

  ```
  command is not allowed when prompts are active
  ```

- Check to see if there is already a background process in progress. If there is a process, the command fails, displaying the following error:

  ```
  previous autoload command is still in progress
  ```

- Check to see if an earlier **ivr autoload url** command has already been configured. If an **ivr autoload** command has already been configured, the user sees the following response when the command is issued:

  ```
  previous command is being replaced
  ```

- When the **no ivr autoload url** command is issued, If there is already an **ivr autoload url** command in progress, it is aborted.

The audio files (prompts) loaded using the **ivr autoload** command are not dynamically swapped out of memory. They are considered as autoloaded prompts as opposed to "dynamic" prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)

Examples

The following example loads audio files from the TFTP server (located at //jurai/mgindi/tclware/index4):

```
ivr autoload url tftp://jurai/mgindi/tclware/index4
```

The following example shows the resulting index file:

```
more index4
tftp://jurai/mgindi/tclware/au/en/en_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

ivr contact-center

To enable a specific set of debug commands on a Cisco router that is being used in a contact center, use the **ivr command-cente**r command in global configuration mode. To stop automatically enabling these debug commands after the router is reloaded, use the **no** form of this command.

ivr command-center

no ivr command-center

Syntax Description

This command has no arguments or keywords.

Command Default

Specific individual debug commands must be manually enabled each time the router is reloaded.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(15)T4	The ccapi, cch323, and ccsip error debugs were included in the output display.
12.4(20)YA	This command was integrated into Cisco IOS Release 12.4(20)YA.

Usage Guidelines

To troubleshoot a Cisco router that is being used in a contact center, it is often necessary to enable specific debug commands to display error messages. Typically, you must manually enable the individual debug commands each time the router is reloaded. Use the **ivr contact-center** command to enable the following debug commands and to automatically re-enable these commands each time the router is reloaded:

- **debug ccsip error**
- **debug cch323 error**
- **debug http client error**
- **debug mrcp error**
- **debug rtsp error**
- **debug voip application error**
- **debug voip application vxml error**
- **debug voice ccapi error**

While this command is configured, the listed debug commands cannot be disabled. Attempts to disable any of these debug commands while the **ivr contact-center** command is configured will display a warning message and the debug command will not be disabled.

Configuring the **no ivr contact-center** command does not disable the listed debug commands. To disable these debug commands after configuring the **no ivr contact-center** command, you must either manually disable each individual debug command or reload the router, after which these debug commands are not re-enabled.

You can verify that the listed debug commands are enabled after you configure the **ivr contact-center** command by using the **show debug** command.

Examples

The following partial output from the **show running-config** command shows that the **ivr contact-center** command is enabled:

```
Router# show running-confi
Building configuration...

Current configuration : 20256 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname c5400-02
!
! ***** snipped *****
!
ivr contact-center
ivr prompt memory 16384 files 1000
ivr asr-server rtsp://CVPASR/media/speechrecognizer
ivr tts-server rtsp://CVPTTS/media/speechsynthesizer
!
! ***** snipped *****
```

The following output from the **show debug** command displays current debugging information that includes the error debug messages automatically enabled by the **ivr contact-center**command:

To display current debugging information that includes the error debug messages automatically enabled by "ivr contact-center", use the show debug command in privileged EXEC mode.

```
c3825-01(config)#ivr contact-center
c3825-01(config)#end
Router# show debug

CCH323 SPI: Error debug is enabled
CCAPI:
  debug voip ccapi error call is ON (filter is OFF)
  debug voip ccapi error software is ON
CCSIP SPI: SIP error debug tracing is enabled   (filter is OFF)

HTTP Client:
  HTTP Client Error debugging is on
APPLICATION:
  debug voip application error is ON

RTSP:
  RTSP client Protocol Error debugging is on
MRCP:
  MRCP client error debugging is on
VXML:
  debug voip application vxml error software is ON
  debug voip application vxml error call is ON (filter is OFF)
c3825-01#
```

Related Commands

Command	Description
debug http client error	Displays error messages for the HTTP client.
debug mrcp error	Displays error messages for Media Resource Control Protocol (MRCP) operations.
debug rtsp error	Displays debug information about the Real-Time Streaming Protocol (RTSP) client.
debug voip application error	Displays error messages for all voice applications.
debug voip application vxml error	Displays error messages for a VoiceXML application.
debug voice ccapi error	Displays error messages for the call control application programming interface (CCAPI) contents.
debug ccsip error	Displays Session Initiation Protocol (SIP)-related error messages.
debug cch323 error	Displays error messages for components within the H.323 subsystem.
show debug	Displays current debugging information automatically enabled by **ivr contact-center** command.

ivr language link

To link configured language packages, use the **ivr language link** command in global configuration mode. To delink the configured language packages, use the **no** form of this command.

ivr language link {**all** | **on-demand**}

no ivr language link

Syntax Description

all	Links all the configured language packages.
on-demand	Links the language packages when asked for.

Command Modes

Global configuration (config)

Command Default

The language packages are not linked.

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to link all the configured language packages:

```
Router# configure terminal
Router(config)# ivr language link all
```

Related Commands

Command	Description
ivr asr-server	Specifies the location of an external media server that provides ASR functionality to voice applications.

ivr prompt cutoff-threshold

To configure the maximum delay time for audio prompts, use the **ivr prompt cut-off threshold** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ivr prompt cutoff-threshold *time*

no ivr prompt cutoff-threshold

Syntax Description

time	Maximum delay time, in milliseconds (ms). The range is from 120 to 1000.

Command Default The maximum delay time is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples The following example shows how to configure the maximum delay time for audio prompts:

```
Router# configure terminal
Router(config)# ivr prompt cutoff-threshold 129
```

Related Commands

Command	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr prompt streamed

To stream audio prompts from particular media types during playback, use the **ivr prompt streamed** command in global configuration mode. To reset to the default, use the **no** form of this command.

Cisco IOS Release 12.4(20)T and Later Releases

ivr prompt streamed {**all** | **flash** | **http** | **none**}

no ivr prompt streamed {**all** | **flash** | **http** | **none**}

Cisco IOS Release 12.4(15)XZ and Earlier Releases

ivr prompt streamed {**all** | **flash** | **http** | **none** | **tftp**}

no ivr prompt streamed {**all** | **flash** | **http** | **none** | **tftp**}

Syntax Description

all	All audio prompts, from all URL types (Flash memory, HTTP).
flash	Audio prompts from Flash memory.
http	Audio prompts from an HTTP URL. This is the default value.
none	No audio prompts from any media type.
tftp	Audio prompts from a TFTP URL. **Note** Only available in Cisco IOS Release 12.4(15)XZ and earlier releases.

Command Default

Audio prompts from HTTP URLs and other media types are not streamed during playback.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The command default was changed from streaming for audio prompts during playback to no streaming.
12.4(20)T	The **tftp** keyword was removed.

Usage Guidelines

To enable streaming for multiple media types, either enter this command for each URL type or enter the ivr prompt streamed all command. If you do not enter this command, audio prompts from HTTP servers and Flash servers are not streamed during playback.

Note Prompts from a Real Time Streaming Protocol (RTSP) server are not controlled by this command and are always streamed during playback.

Examples

The following example indicates that audio prompts from Flash memory are streamed when they are played back:

```
ivr prompt streamed flash
```

Related Commands

Command	Description
ivr prompt memory	Sets the maximum amount of memory that dynamic audio prompts can occupy in memory.

ivr record cpu flash

To configure the maximum percentage allowed for the flash write process in CPU, use the **ivr record cpu flash** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ivr record cpu flash *number*

no ivr record cpu flash

Syntax Description

number	Numeric label that specifies the maximum percentage allowed for the flash write process in the CPU. The range is from 1 to 99. The default is 99.

Command Default

The maximum percentage is configured to 99.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows that the flash recording allowed is set to 50 percent:

```
Router# configure terminal
Router(config)# ivr record cpu flash 50
```

Related Commands

Caommand	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr record memory session

To set the maximum amount of memory that can be used to record voice messages during a single call session, use the **ivr record memory session** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory session *kilobytes*

no ivr record memory session

Syntax Description

kilobytes	Memory size, in kilobytes. Range is 0 to 256000. The default is 256.

Command Default

256 KB

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum memory allowed for audio recordings during a single call session on a VoiceXML-enabled gateway.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the maximum memory limit to 512 KB for a single call session:

```
ivr record memory session 512
```

Related Commands

Command	Description
ivr record memory system	Sets the maximum amount of memory that can be used to store all voice recordings on the VoiceXML-enabled gateway.

ivr record memory system

To set the maximum amount of memory that can be used to store all voice recordings on the gateway, use the **ivr record memory system** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory system *kilobytes*

no ivr record memory system

Syntax Description

kilobytes	Memory limit, in kilobytes. Range is 0 to 256000. If 0 is configured, the RAM recording function is disabled on the gateway. The default for Cisco 3640 and Cisco AS5300 is 10000. The default for Cisco 3660, Cisco AS5350, and Cisco AS5400 is 20000.

Command Default

Cisco 3640 and Cisco AS5300: 10,000 KB
Cisco 3660, Cisco AS5350, and Cisco AS5400: 20,000 KB

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum amount of gateway memory that is used for storing all voice recordings.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the total memory limit for all recordings to 8000 KB:

```
ivr record memory system 8000
```

Related Commands

Command	Description
ivr record memory session	Sets the maximum amount of memory that can be used to record voice messages during a single call session.

ivr tts-server

To specify the location of an external media server that provides text-to-speech (TTS) functionality to voice applications, use the **ivr tts-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr tts-server *url*

no ivr tts-server

Syntax Description

url	Location of the TTS resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr tts-server rtsp://*host***:***port***/synthesizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr tts-server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the *Cisco VoiceXML Programmer's Guide*.

To specify the voice profile that the TTS server uses for voice synthesis operations, use the **ivr tts-voice-profile** command.

Examples

The following example specifies that voice applications use the TTS server named "tts_serv":

```
Router(config)# ivr tts-server rtsp://tts_serv/synthesizer
```

The following example specifies that voice applications use the MRCP v2 TTS server named "tts_mrcpv2serv":

```
Router(config)# ivr tts-server sip:tts_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr asr-server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts-voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr tts-voice-profile

To specify the location of the voice profile that is used by text-to-speech (TTS) servers, use the **ivr tts-voice-profile** command in global configuration mode. To remove the voice profile, use the **no** form of this command.

ivr tts-voice-profile *url*

no ivr tts-voice-profile

Syntax Description

url	Location of the TTS voice profile file, in URL format.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines This command specifies the voice profile that a TTS server uses for voice synthesis operations. The voice profile is a W3C Simple Markup Language (SML) file that specifies voice parameters like gender, speed, and so forth. The TTS server uses this voice profile unless the markup file that it is translating has overriding values.

The TTS voice profile can be stored on an HTTP server or on RTSP, TFTP, or FTP servers if the media sever supports these locations.

The TTS voice profile location can also be specified in the VoiceXML document by using the Cisco proprietary property com.cisco.tts-voice-profile. The VoiceXML property in the document overrides the value that is configured by using this command.

To specify the location of the external media server that is providing TTS functionality, use the **ivr tts-server** command.

Examples The following example tells the TTS server to use the voice profile file named “vprofil2”, which is located on an HTTP server:

```
ivr tts-voice-profile http://ttserver/vprofil2.sml
```

Related Commands

Command	Description
ivr asr-server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts-server	Specifies the media server that provides TTS functionality to IVR applications.

ixi application cme

To enter XML application configuration mode for the Cisco Unified CallManager Express (Cisco Unified CME) application, use the **ixi application cme** command in global configuration mode.

ixi application cme

Syntax Description This command has no arguments or keywords.

Command Default XML parameters are not set for the Cisco Unified CME application.

Command Modes Global configuration (config)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines In Cisco Unified CME 4.0 and later versions, an XML interface is provided through the Cisco IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application itself.

When you are using the Cisco IOS XML Infrastructure, the same HTTP transport layer can be used by multiple applications. The **ixi application cme** command enters XML application configuration mode to allow you to set Cisco IOS XML Infrastructure parameters for the Cisco Unified CME application. In this configuration mode, you can set the response timeout parameter using the **response timeout** command and enable communication with the application using the **no shutdown** command.

The **ixi transport** command allows you to set parameters for the Cisco IOS XML Infrastructure transport layer.

Note The **no** form of the **ixi application cme** command is not supported.

Examples The following example shows how to configure the Cisco Unified CME application to overwrite the Cisco IOS XML Infrastructure transport-level timeout with a 30-second response timeout and enable XML communication with the application.

```
Router(config)# ixi application cme
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# no shutdown
```

Related Commands

Command	Description
ixi transport	Enters XML transport configuration mode.
no shutdown	Enables XML communication with the application.
response (XML application)	Sets a timeout for responding to the XML application and overwrites the IXI transport-level timeout.

ixi application mib

To enter XML application configuration mode, use the **ixi application mib** command in global configuration mode.

ixi application mib

Syntax Description

mib	XML application for which parameters will be configured. Valid value: **mib**.

Command Default No XML applications are configured.

Command Modes Global configuration mode

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applicatiosn in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed.

An eXtensible Markup Language (XML) application programming interface (API) supports Cisco IOS commands allowing you to specify certain parameters associated with the XML API.

Once you are in XML application configuration mode, you can use the following commands:

- **default**—XML application configuration parameters defaults.
- **exit**—Apply changes and exit from XML application configuration mode.
- **help**—Display of the interactive help system.
- **no**—Negate a command or set its defaults.
- **response**—Response parameters.
- **shutdown**—Stop the application.

Examples The following example shows how to enter XML application configuration mode, set the XML application timeout period to 30 seconds, format the response parameters to in human readable XML, and exit XML application configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi application mib
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# response formatted
Router(conf-xml-app)# exit
```

Related Commands

Command	Description
ixi transport http	Sets XML transport parameters.
response (XML application)	Sets XML application mode response parameters.

ixi transport http

To enter XML transport configuration mode, use the **ixi transport** command in global configuration mode.

ixi transport http

Syntax Description

http	Specifies the http transport protocol.

Command Default No XML transport is configured.

Command Modes Global configuration mode

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applications in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed. IXI allows applications to be written in a transport independent manner. The **ixi transport** command enters XML transport configuration mode where you can set transport configuration parameters.

Once you are in XML transport configuration mode, you can access the following commands:

- **default** *option*—XML transport configuration command defaults.
- **exit**—Apply changes and exit from XML application configuration mode.
- **help**—Display the interactive help system.
- **no**—Negate a command or set its defaults.
- **request**—Request handling parameters.
- **response size**—Response transport fragment size.
- **shutdown**—Stop the transport.

Examples The following example shows how to enter XML transport configuration mode, set the XML transport fragment size to 32 Kbytes, and exit XML transport configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi transport http
Router(conf-xml-trans)# response size 32
Router(conf-xml-trans)# exit
```

Related Commands

Command	Description
ixi application mib	Sets XML application parameters.
request (XML transport)	Sets XML transport request handling parameters.
response size (XML transport)	Set the XML transport fragment size.

Cisco IOS Voice Commands: K

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

keepalive retries

To set the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive retries** command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

keepalive retries *number*

no keepalive retries

Syntax Description

number	Number of keepalive attempts. Range is 1 to 32. Default is 3.

Command Default

3 keepalive attempts

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to control the number of keepalive retries before SCCP confirms that the Cisco Unified CallManager link is down. When SCCP confirms that the Cisco Unified CallManager link is down (if the number of keepalive messages sent without receiving an Ack reaches the keepalive retries value), Cisco Unified CallManager switchover is initiated.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the keepalive retries to meet your needs.

Examples

The following example sets the number of times that a Cisco Unified CallManager retries before confirming that the link is down to seven:

```
Router(conf-sccp-ccm)# keepalive retries 7
```

Related Commands

Command	Description
keepalive timeout	Sets the length of time between keepalive messages from SCCP to Cisco Unified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters the SCCP Cisco CallManager configuration mode.

keepalive target

To identify Session Initiation Protocol (SIP) servers that will receive keepalive packets from the SIP gateway, use the **keepalive target** command in SIP user-agent configuration mode. To disable the **keepalive target** command behavior, use the **no** form of this command.

keepalive target {{**ipv4:***address* | **ipv6:***address*}[**:***port*] | **dns:***hostname*} | [**tcp** [**tls**]] | [**udp**] | [**secondary**]

no keepalive target [**secondary**]

Syntax Description

ipv4:*address*	IP address (in IP version 4 format) of the primary or secondary SIP server to monitor.
ipv6:*address*	IPv6 address of the primary or secondary SIP server to monitor.
:*port*	(Optional) SIP port number. Default SIP port number is 5060.
dns:*hostname*	DNS hostname of the primary or secondary SIP server to monitor.
tcp	(Optional) Sends keepalive packets over TCP.
tls	(Optional) Sends keepalive packets over Transport Layer Security (TLS).
udp	(Optional) Sends keepalive packets over User Datagram Protocol (UDP).
secondary	(Optional) Associates the IP version 4 address or the domain name system (DNS) hostname to a secondary SIP server to monitor.

Command Default

No keepalives are sent by default from SIP gateway to SIP gateway. The SIP port number is 5060 by default.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

The primary or secondary SIP server addresses are in the following forms: dns:example.sip.com or ipv4:172.16.0.10.

Examples

The following example sets the primary SIP server address and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
```

The following example sets the primary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
```

The following example sets both the primary and secondary SIP server address and the transport to UDP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 udp
 keepalive target ipv4:172.16.0.20 udp secondary
```

The following example sets both the primary and secondary SIP server addresses and defaults to the UDP transport:

```
sip-ua
 keepalive target ipv4:172.16.0.10
 keepalive target ipv4:172.16.0.20 secondary
```

The following example sets the primary SIP server address and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp
 keepalive target ipv4:172.16.0.20 tcp secondary
```

The following example sets the primary SIP server address and the transport to TCP and sets security to TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
```

The following example sets both the primary and secondary SIP server addresses and the transport to TCP and sets security to the TLS mode:

```
sip-ua
 keepalive target ipv4:172.16.0.10 tcp tls
 keepalive target ipv4:172.16.0.20 tcp tls secondary
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive trigger	Sets the trigger count to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
retry keepalive	Sets the retry keepalive count for retransmission.
timers keepalive	Sets the timers keepalive interval between sending Options message requests when the SIP server is active or down.

keepalive timeout

To set the length of time between keepalive messages from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive timeout** command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the **no** form of this command.

keepalive timeout *seconds*

no keepalive timeout

Syntax Description

seconds	Time between keepalive messages. Range is 1 to 180. Default is 30.

Command Default

30 seconds

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Whenever SCCP sends the keepalive message to the Cisco Unified CallManager, it initiates this timer. Once the timeout occurs, it sends the next keepalive message unless the number of keepalive (messages without an Ack) reaches the number set by the **keepalive retries** command. As of now, the SCCP protocol uses the value provided by the Cisco Unified CallManager.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the keepalive timeout value to meet your needs.

Examples

The following example sets the length of time between Cisco Unified CallManager keepalive messages to 120 seconds (2 minutes):

```
Router(config-sccp-ccm)# keepalive timeout 120
```

Related Commands

Command	Description
keepalive retries	Sets the number of keepalive retries from SCCP to Cisco Unified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.

keepalive trigger

The trigger interval (in seconds) represent the number of Options message requests that must consecutively receive responses from the SIP servers when in the down state in order to unbusy the voice ports, use the **keepalive trigger** command in SIP UA configuration mode. To restore to the default value of 3 seconds, use the **no** form of this command.

keepalive trigger *seconds*

no keepalive trigger *seconds*

Syntax Description

seconds	Keepalive trigger value in the range from 1 to 10 seconds. The default value is 3 seconds.

Command Default

The default value for the keepalive trigger is 3 seconds.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Sets the time interval (in seconds) to represent the number of Options message requests that must be consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state. The keepalive trigger interval is measured in seconds. The default is 3 seconds.

Examples

The following example sets a time interval (in seconds) after the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state. The trigger interval is set to 8 seconds in the following example:

```
sip-ua
 keepalive trigger 8
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
retry keepalive	Sets the retry keepalive interval for retransmission.
timers keepalive	Sets the time interval between sending Options message requests when the SIP server is active or down.

Cisco IOS Voice Commands: L

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

link (RLM)

To enable a Redundant Link Manager (RLM) link, use the **link** command in RLM configuration mode. To disable this function, use the **no** form of this command.

link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*

no link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*

Syntax Description

hostname ***name***	RLM host name. If host name is used, RLM looks up the DNS server periodically for the host name configured until lookup is successful or the configuration is removed.
address *ip-address*	IP address of the link.
source *loopback-source*	Loopback interface source. We recommend that you use the loopback interface as the source, so that it is independent of the hardware condition. Also, the source interface should be different in every link to avoid falling back to the same routing path. If you intend to use the same routing path for the failover, a single link is sufficient to implement it.
weight *factor*	An arbitrary number that sets link preference. The higher the weighting factor number assigned, the higher priority it gets to become the active link. If all entries have the same weighting factor assigned, all links are treated equally. There is no preference among servers according to the assumption that only one server accepts the connection requests at any given time. Otherwise, preferences are extended across all servers.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

This command is a preference-weighted multiple entries command. Within the same server, the link preference is specified in weighting.

Examples

The following example specifies the RLM group (network access server), device name, and link addresses and their weighting preferences:

```
rlm group 1
 server r1-server
  link address 10.1.4.1 source Loopback1 weight 4
  link address 10.1.4.2 source Loopback2 weight 3
```

listen-port (SIP)

To manually change the defined Session Initiation Protocol (SIP) listen port for UDP/TCP/TLS calls, use the **listen-port** command in SIP configuration mode. To reset the UDP/TCP/TLS port to the default value, use the **no** form of this command.

listen-port {**secure** | **non-secure**} *port-number*

no listen-port non-secure

Syntax Description

secure	Specifies the TLS port value.
non-secure	Specified the TCP/UDP port value.
port-number	Port number. Range: 1 to 65535. The default for UDP/TCP is 5060; the default for TLS is 5061.

Command Default

The port number is set to the default value based on the transport layer protocol used.

Command Modes

SIP configuration mode (config-serv-sip)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **listen-port** command is configurable on both incoming and outgoing SIP calls, and is applicable for both TDM-IP gateway and Cisco Unified Border Element (Cisco Unified BE) (previously known as IPIPGW). The Cisco UBE gateway port number defined in global configuration will be used for both In leg and Out leg. Before configuring the SIP listen port for TCP/UDP/TLS, SIP service should be shut down using the **shutdown** in SIP configuration mode. If SIP service is not shut down, the **listen-port** command flashes an error message saying “shutdown SIP service before changing SIP listen port”. This ensures that there are no active calls when the SIP listen port is changed. The **non-secure** keyword is supported on non-Crypto images, and both the **secure** and **non-secure** keywords are supported on Crypto images.

The following restrictions apply:

- Configuring the SIP listen port on a dial-peer basis is not supported.
- Configuring same listening port for both UDP/TCP and TLS is not allowed.
- Configuring the SIP listen port to a port that is already in use is not supported and results in an error message.
- Changing SIP listen port when Transport services (TCP/UDP/TLS) are shut down, will not close or reopen the port. The result is that only the new port number is updated. The new port will be bound when Transport services (TCP/UDP/TLS) is enabled.

Examples

The following example shows the port number on a Crypto image being changed to port 2000:

```
Router(config-serv-sip)# listen-port secure 2000
```

The following example shows the port number being reset to the TLS default port:

```
Router(config-serv-sip)# no listen-port
```

Related Commands

Command	Description
shutdown	Disables the port.

lmr duplex half

To have the voice path for a voice port operate in half duplex mode, use the **lmr duplex half** command in voice-port configuration mode. To return to the default, use the **no** form of this command.

lmr duplex half

no lmr duplex half

Syntax Description This command has no arguments or keywords.

Command Default Full duplex mode

Command Modes Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines When a radio system is receiving voice traffic from the radio, operating the voice path in half duplex mode prevents the speaker from being interrupted and prevents the voice stream from being fed back to itself.

Examples In the following example, the voice path for voice port 1/0/0 on a Cisco 3700 series router is set to operate in half duplex mode:

```
voice-port 1/0/0
 lmr duplex half
```

lmr e-lead

To define the use of the E-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr e-lead** command in voice-port configuration mode. To return to the default use of the E-lead, use the **no** form of this command.

lmr e-lead {**inactive** | **seize** | **voice**}

no lmr e-lead {**inactive** | **seize** | **voice**}

Syntax Description

inactive	Specifies that the router never sends a seize signal on the E-lead to the LMR device. The router sends voice packets to LMR devices.
seize	Specifies that for PLAR and multicast connections, the router sends a seize signal on the E-lead when the LMR port is connected and removes the seize signal from the E-lead when the LMR port is not involved in a VoIP connection. This is the default. Specifies that for connection trunk connections, the router does not send a seize signal when the LMR port is connected. Instead, if the trunk connection is up, the M-lead signal from the far-end router is passed through as the E-lead on the near-end router. When the M-lead is dropped on the far-end router and the trunk connection is still up, the E-lead is dropped on the near-end router.
voice	Specifies that the router sends a seize signal on the E-lead only when it receives voice packets from the network. When no packets are detected on the network, the seize signal is removed from the E-lead.

Command Default

seize

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under E-lead control. Use the **lmr e-lead** command to configure the voice port when using private line, automatic ringdown (PLAR) connections. The E-lead connects to the Push To Talk (PTT) of the LMR system.

Examples

In the following example, packet transmission from the E&M voice port on a Cisco 3745 to an attached LMR radio system is disabled:

```
lmr e-lead inactive
```

Related Commands

Command	Description
lmr m-lead	Defines the use of the M-lead in signaling between the E&M voice port on the router and the attached LMR device.

lmr ip-vad

To configure the Land Mobile Radio (LMR) digital signal processor (DSP) on a Cisco 2800 series integrated services router to report a voice packet arrival event only if the packet contains voice energy, use the **lmr ip-vad** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

lmr ip-vad

no lmr ip-vad

Syntax Description

This command has no arguments or keywords.

Command Default

Any voice packet received from the IP network side triggers the DSP to report a voice packet arrival event to the Cisco IOS software.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **lmr ip-vad** command applies to a voice interface card (VIC) in a Cisco 2800 series integrated services router if the VIC is one of the following types of ear and mouth (E&M) interfaces:

- VIC2-2E/M with signal type LMR
- ds0-group created with signal type e&m-lmr under an E1 or T1 controller

The **lmr ip-vad** command configures the LMR DSP to report voice activity detection (VAD) status change events (rather than voice packet arrival events) for a supported voice interface in a Cisco 2800 series integrated services router.

Examples

The following example shows a sequence of commands that can be used to configure a voice port so that a voice packet arrival event is reported to the Cisco IOS software on the router only if the packet contains voice energy.

```
Router(config)# voice-port 1/1/0
Router(config-voiceport)# signal lmr
Router(config-voiceport)# lmr ip-vad
```

Related Commands

Command	Description
signal	Configures the type of signaling to be used for a voice port.
voice-port	Enters voice-port configuration mode.

lmr led-on

To use the ear and mouth (E&M) LED to indicate the E-lead and M-lead status, use the **lmr led-on** command in voice-port configuration mode. To return to the default use of the E&M LED, use the **no** form of this command.

lmr led-on

no lmr led-on

Syntax Description

This command has no arguments or keywords.

Command Default

The E&M LED indicates voice port activity only.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command is available on an E&M voice port only if the signal type for that port is Land Mobile Radio (LMR). This command enables the use of the E&M LED to indicate the E-lead and M-lead status as follows:

- Red—E-lead active
- Green—M-lead active
- Yellow—Both E-lead and M-lead active

The default behavior of the E&M LED is to light up when there is activity on the voice port and to turn off when there is no activity.

Examples

The following example specifies that the E&M LED is used to indicate the E-lead and M-lead status:

```
voice-port 1/0/0
 lmr led-on
```

lmr m-lead

To define the use of the M-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr m-lead** command in voice-port configuration mode. To return to the default use of the M-lead, use the **no** form of this command.

lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}

no lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}

Syntax Description

inactive	The router ignores signals sent by voice on the M-lead. The flow of voice packets is determined by voice activity detection (VAD). The router sends voice received from the LMR device. This is the default.
audio-gate-in	The router generates VoIP packets when a seize signal is detected on the M-lead. The router stops generating VoIP packets when the seize signal is removed from the M-lead.
dialin	When the LMR device is not involved in a VoIP connection, the first seize signal detected on the M-lead triggers the router to set up a VoIP connection. Once the connection is made, the router behaves as in the **audio-gate-in** option.

Command Default

inactive

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr m-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under M-lead control. The M-lead corresponds to the Carrier Operated Relay (COR) of the LMR system, which indicates receive activity on the LMR system.

Examples

In the following example, an LMR radio system attached to the E&M voice port on a Cisco 3745 is allowed to transmit audio by first raising the E-lead, then transmitting:

```
lmr m-lead dialin
```

Related Commands

Command	Description
lmr e-lead	Defines the use of the E-lead in signaling between the E&M voice port on the router and the attached LMR device.

load-balance

To configure load balancing, use the **load-balance** command in gatekeeper configuration mode. To disable load balancing, use the **no** form of this command.

load-balance [**endpoints** *max-endpoints*] [**calls** *max-calls*] [**cpu** *max-%cpu*] [**memory** *max-%mem-used*]

no load-balance [**endpoints** *max-endpoints*] [**calls** *max-calls*] [**cpu** *max-%cpu*] [**memory** *max-%mem-used*]

Syntax Description

endpoints *max-endpoints*	(Optional) Maximum number of endpoints.
calls *max-calls*	(Optional) Maximum number of calls.
cpu *max-%cpu*	(Optional) Maximum percentage of CPU utilization.
memory *max-%mem-used*	(Optional) Maximum percentage of memory used.

Command Default

Load balancing is performed by the gatekeeper.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

Load balancing occurs when one gatekeeper reaches the default or the configured load level. Upon reaching the load-level threshold, the gatekeeper begins sending alternate gatekeeper information in Registration, Admission, and Status (RAS) messages, and the gateways then attempt to migrate from the loaded gatekeeper to its least busy alternate. The move is permanent; endpoints are not actively moved back to the original gatekeeper if it stabilizes. However, they may return to that gatekeeper if the new gatekeeper reaches a load threshold and transfers them again. The gatekeepers share the load, but they may not have equal shares. The process of load balancing allows for more effective zone management.

Examples

The following example configures load balancing:

```
load-balance endpoints 200 calls 100 cpu 75 memory 80
```

Related Commands

Command	Description
zone cluster local	Configures alternate gatekeepers for each zone.

local

To define the local domain, including the IP address and port that the border element (BE) should use for interacting with remote BEs, use the **local** command in Annex G configuration mode. To reset to the default, use the **no** form of this command.

local ip *ip-address* [**port** *local-port*]

no local ip

Syntax Description

ip *ip-address*	IP address of the local border element.
port *local-port*	(Optional) Port number of the local border element, which is used for exchanging Annex G messages. Default is 2099.

Command Default Port number: 2099

Command Modes Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The local IP address can be a virtual Hot Standby Routing Protocol (HSRP) address for high reliability and availability. You can configure multiple gatekeepers and BEs identically and use HSRP to designate a primary BE and other standby BEs. If the primary BE is down, a standby BE operates in its place.

Examples The following example sets the IP address and port that the BE should use. (Note that this example uses a nonstandard port number. If you do not want to use a nonstandard port number, use the default value of 2099.)

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# local ip 121.90.10.80 port 2010
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
show call-router status	Displays the Annex G BE status.

localhost

To globally configure Cisco IOS voice gateways, Cisco Unified Border Elements (Cisco UBEs), or Cisco Unified Communications Manager Express (Cisco Unified CME) to substitute a Domain Name System (DNS) hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **localhost** command in voice service SIP configuration mode. To remove a DNS localhost name and disable substitution for the physical IP address, use the **no** form of this command.

localhost dns:[*hostname.*]*domain* [**preferred**]

no localhost

Syntax Description

dns:[*hostname.*]*domain*	Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages. This value can be the hostname and the domain separated by a period (**dns:***hostname.domain*) or just the domain name (**dns:***domain*). In both case, the **dns:** delimiter must be included as the first four characters.
preferred	(Optional) Designates the specified DNS hostname as preferred.

Command Default

The physical IP address of the outgoing dial peer is sent in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)XA	This command was modified. The **preferred** keyword was added to specify the preferred localhost if multiple registrars are configured on a SIP trunk.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.

Usage Guidelines

Use the **localhost** command in voice service SIP configuration mode to globally configure a DNS localhost name to be used in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on Cisco IOS voice gateways, Cisco UBEs, or Cisco Unified CME. When multiple registrars are configured you can then use the **localhost preferred** command to specify which host is preferred.

To override the global configuration and specify DNS localhost name substitution settings for a specific dial peer, use the **voice-class sip localhost** command in dial peer voice configuration mode. To remove a globally configured DNS localhost name and use the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **no localhost** command.

Examples

The following example shows how to globally configure a preferred DNS localhost name using only the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:example.com preferred
```

The following example shows how to globally configure a preferred DNS localhost name by specifying the hostname along with the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:MyHostname.example.com preferred
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

loopback (controller)

To set the loopback method for testing a T1 or E1 interface, use the **loopback** command in controller configuration mode. To reset to the default, use the **no** form of this command.

loopback {**diagnostic** | **local** {**payload** | **line**} | **remote** {**v54 channel-group** *channel-number* | **iboc** | **esf** {**payload** | **line**}}}

no loopback

Syntax Description

diagnostic	Loops the outgoing transmit signal back to the receive signal.
local	Places the interface into local loopback mode.
payload	Places the interface into external loopback mode at the payload level.
line	Places the interface into external loopback mode at the line level.
remote	Keeps the local end of the connection in remote loopback mode.
v54 channel-group	Activates a V.54 channel-group loopback at the remote end. Available for both T1 and E1 facilities.
channel-number	Channel number for the V.54 channel-group loopback. Range is from 0 to 1.
iboc	Sends an inband bit-oriented code to the far end to cause it to go into line loopback.
esf	T1 or E1 frame type of Extended Super Frame (ESF). Only available under T1 or E1 controllers when ESF is configured on the controller. The following are keywords: • **payload**—Activates remote payload loopback by sending Facility Data Link (FDL) code. FDL is a 4-kbps out-of-band signaling channel in ESF. • **line**—Activates remote line loopback by sending FDL code.

Command Default No loopback is configured.

Command Modes Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced as a controller configuration command for the Cisco MC3810.
12.0(5)T and 12.0(5)XK	The command was introduced as an ATM interface configuration command for the Cisco 2600 series and Cisco 3600 series.
12.0(5)XE	The command was introduced as an ATM interface configuration command for the Cisco 7200 series and Cisco 7500 series.
12.0(5)XK and 12.0(7)T	The command was introduced as a controller configuration command for the Cisco 2600 series and Cisco 3600 series.
12.1(1)T	The command was modified as a controller configuration command for the Cisco 2600 series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused either by the line and channel service unit/digital service unit (CSU/DSU) or by the interface. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example sets the diagnostic loopback method on controller T1 0/0:

```
controller t1 0/0
 loopback diagnostic
```

The following example sets the payload loopback method on controller E1 0/0:

```
controller e1 0/0
 loopback local payload
```

loop-detect

To enable loop detection for T1, use the **loop-detect** command in controller configuration mode. To cancel loop detection, use the **no** form of this command.

loop-detect

no loop-detect

Syntax Description

This command has no arguments or keywords.

Command Default

Loop detection is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example configures loop detection for controller T1 0:

```
controller t1 0
 loop-detect
```

Related Commands

Command	Description
loopback (interface)	Diagnoses equipment malfunctions between an interface and a device.

loss-plan

To specify the analog-to-digital gain offset for an analog Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **loss-plan** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

loss-plan {**plan1** | **plan2** | **plan3** | **plan4** | **plan5** | **plan6** | **plan7** | **plan8** | **plan9**}

no loss-plan

Syntax Description

plan1	FXO: A-D gain = 0 dB, D-A gain = 0 dB. FXS: A-D gain = –3 dB, D-A gain = –3 dB.
plan2	FXO: A-D gain = 3 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = –3 dB.
plan3	FXO: A-D gain = –3 dB, D-A gain = 0 dB. FXS: Not applicable.
plan4	FXO: A-D gain = –3 dB, D-A gain = –3 dB. FXS: Not applicable.
plan5	FXO: Not applicable. FXS: A-D gain = –3 dB, D-A gain = –10 dB.
plan6	FXO: Not applicable. FXS: A-D gain = 0 dB, D-A gain = –7 dB.
plan7	FXO: A-D gain = 7 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = –6 dB.
plan8	FXO: A-D gain = 5 dB, D-A gain = –2 dB. FXS: Not applicable.
plan9	FXO: A-D gain = 6 dB, D-A gain = 0 dB. FXS: Not applicable.

Command Default

FXO: A-D gain = 0 dB, D-A gain = 0 dB (loss plan 1)
FXS: A-D gain = –3 dB, D-A gain = –3 dB (loss plan 1)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	The following additional signal level choices were added: plan 3, plan 4, plan 8, and plan 9.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command sets the analog signal level difference (offset) between the analog voice port and the digital signal processor (DSP). Each loss plan specifies a level offset in both directions—from the analog voice port to the DSP (A-D) and from the DSP to the analog voice port (D-A).

Use this command to obtain the required levels of analog voice signals to and from the DSP.

Examples

The following example configures FXO voice port 1/6 for a –3 dB offset from the voice port to the DSP and for a 0 dB offset from the DSP to the voice port:

```
voice-port 1/6
 loss-plan plan3
```

The following example configures FXS voice port 1/1 for a 0 dB offset from the voice port to the DSP and for a –7 dB offset from the DSP to the voice port:

```
voice-port 1/1
 loss-plan plan6
```

Related Commands

Command	Description
impedance	Specifies the terminating impedance of a voice port interface.
input gain	Specifies the gain applied by a voice port to the input signal from the PBX or other customer premises equipment.
output attenuation	Specifies the attenuation applied by a voice port to the output signal toward the PBX or other customer premises equipment.

lrq e164 early-lookup

To start the E.164 registered endpoint matching before via-zone routing is processed in the location request (LRQ) routing process, use the **lrq e164 early-lookup** command in gatekeeper configuration mode. To return to the default behavior, use the **no** form of this command.

lrq e164 early-lookup

no lrq e164 early-lookup

Syntax Description This command has no arguments or keywords.

Command Default The E.164 endpoint matching is done at the last stage of LRQ routing.

Command Modes Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines The default gatekeeper algorithm for IP-to-IP gateway selection is based on the via-zone prefix and tech-prefix match. Use the **lrq e164 early-lookup** command to start the E.164 matching process before via-zone routing to block nonregistered endpoints.

Examples The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)# gatekeeper
Router(config-gk)# lrq e164 early-lookup
```

lrq forward-queries

To enable a gatekeeper to forward location request (LRQ) messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers, use the **lrq forward-queries** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq forward-queries

no lrq forward-queries

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines LRQ forwarding is dependent on a Cisco nonstandard field that first appeared in Cisco IOS Release 12.0(3)T. This means that any LRQ message received from a non-Cisco gatekeeper or any gatekeeper running a Cisco IOS software image prior to Cisco IOS Release 12.0(3)T is not forwarded.

The routing of E.164-addressed calls is dependent on the configuration of zone prefix tables (for example, area code definitions) on each gatekeeper. Each gatekeeper is configured with a list of prefixes controlled by itself and by other remote gatekeepers. Calls are routed to the zone that manages the matching prefix. Thus, in the absence of a directory service for such prefix tables, you, the network administrator, may have to define extensive lists of prefixes on all the gatekeepers in your administrative domain.

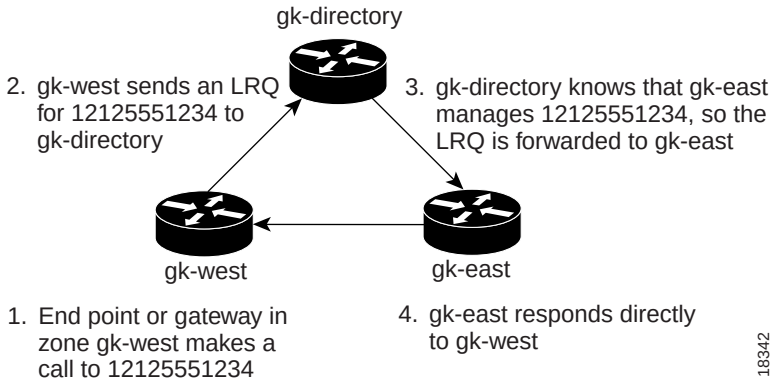
To simplify this task, you can select one of your gatekeepers as the "directory" gatekeeper and configure that gatekeeper with the complete list of prefixes and the **lrq forward-queries** command. You can then simply configure all the other gatekeepers with their own prefixes and the wildcard prefix "*" for your directory gatekeeper.

This command affects only the forwarding of LRQ messages for E.164 addresses. LRQ messages for H.323-ID addresses are never forwarded.

Examples

The following example selects one gatekeeper as the directory gatekeeper. See Figure 6.

Figure 6 Example Scenario with Directory Gatekeeper and Two Remote Gatekeepers



Configuration on gk-directory

On the directory gatekeeper called gk-directory, identify all the prefixes for all the gatekeepers in your administrative domain:

```
zone local gk-directory cisco.com
zone remote gk-west cisco.com 172.16.1.1
zone remote gk-east cisco.com 172.16.2.1

zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......

zone prefix gk-east 1212.......
zone prefix gk-east 1617.......

lrq forward-queries
```

Configuration on gk-west

On the gatekeeper called gk-west, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-west cisco.com
zone remote gk-directory cisco.com 172.16.2.3

zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......
zone prefix gk-directory *
```

Configuration on gk-east

On the gatekeeper called gk-east, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-east cisco.com
zone remote gk-directory cisco.com 172.16.2.3

zone prefix gk-east 1212.......
zone prefix gk-east 1617.......
zone prefix gk-directory *
```

When an endpoint or gateway in zone gk-west makes a call to 12125551234, gk-west sends an LRQ message for that E.164 address to gk-directory, which forwards the message to gk-east. Gatekeeper gk-east responds directly to gk-west.

Related Commands

Command	Description
lrq reject-unknown-prefix	Enables the gatekeeper to reject all LRQ messages for zone prefixes that are not configured.

lrq lrj immediate-advance

To enable the Cisco IOS gatekeeper to immediately send a sequential location request (LRQ) message to the next zone after it receives a location reject (LRJ) message from a gatekeeper in the current zone, use the **lrq lrj immediate-advance** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq lrj immediate-advance

no lrq lrj immediate-advance

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(4)T	This command was introduced. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.

Usage Guidelines

In a network in which LRQ messages are forwarded through multiple gatekeepers along a single path, a single LRQ message sent from a gatekeeper could solicit multiple LRJ and location confirmation (LCF) responses. If an LRJ response is received first, a potentially unnecessary LRQ message could be sent to the next zone, increasing traffic.

To avoid this problem, perform the following:

- Configure the zone prefix to send sequential LRQ messages rather than to use the **blast** option, using the **zone prefix** command.
- Configure the sequential timer on each gatekeeper along the path, using the **timer lrq seq delay** command.

Examples

The following example enables the gatekeeper to immediately send a sequential LRQ message to the next zone after it receives an LRJ message from a gatekeeper in the current zone.

```
lrq lrj immediate-advance
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive sequential LRQ messages.
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQ messages.
zone prefix	Adds a prefix to the gatekeeper zone list.

lrq reject-resource-low

To configure a gatekeeper to notify a sending gatekeeper on receipt of a location request (LRQ) message that no terminating endpoints are available, use the **lrq reject-resource-low** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq reject-resource-low

no lrq reject-resource-low

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco 7400 series.

Examples

The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)# gatekeeper
Router(config-gk)# lrq reject-resource-low
```

lrq reject-unknown-circuit

To enable the gatekeeper to reject a location request (LRQ) message that contains an unknown destination circuit, use the **lrq reject-unknown-circuit** command in gatekeeper configuration mode. To disable the rejection, use the **no** form of this command.

lrq reject-unknown-circuit

no lrq reject-unknown-circuit

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The gatekeeper checks the destination circuit field in each LRQ message. If the field contains a circuit unknown to the gatekeeper and this command is entered, the gatekeeper rejects the LRQ request. If this command is disabled, the gatekeeper tries to resolve the alias without considering the circuit.

Examples

The following example causes the gatekeeper to reject unknown carriers in an LRQ request:

```
Router(config)# gatekeeper
Router(config-gk)# lrq reject-unknown-circuit
```

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

lrq reject-unknown-prefix

To enable the gatekeeper to reject all location request (LRQ) messages for zone prefixes that are not configured, use the **lrq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming LRQ messages, use the **no** form of this command.

lrq reject-unknown-prefix

no lrq reject-unknown-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

The gatekeeper accepts and processes all incoming LRQ messages.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use this command to configure the gatekeeper to reject any incoming LRQ messages for a destination E.164 address that does not match any of the configured zone prefixes.

Whether or not you use this command, the following is true when the E.164 address matches a zone prefix:

- If the matching zone prefix is local (that is, controlled by this gatekeeper), the LRQ message is serviced.
- If the matching zone prefix is remote (that is, controlled by some other gatekeeper), the LRQ message is rejected.

If you do not use this command and the target address does not match any known local or remote prefix, the default behavior is to attempt to service the call using one of the local zones. If this default behavior is not suitable for your site, use this command on your router to force the gatekeeper to reject such requests.

Examples

Consider the following gatekeeper configuration:

```
zone local gk408 cisco.com
zone local gk415 cisco.com
zone prefix gk408 1408.......
zone prefix gk415 1415.......
lrq reject-unknown-prefix
```

In this sample configuration, the gatekeeper is configured to manage two zones. One zone contains gateways with interfaces in the 408 area code, and the second zone contains gateways in the 415 area code. Then using the **zone prefix** command, the gatekeeper is configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

Now say some other zone has been erroneously configured to route calls to the 212 area code to this gatekeeper. When the LRQ message for a number in the 212 area code arrives at this gatekeeper, the gatekeeper fails to match the area code, and the message is rejected.

If this was your only site that had any gateways in it and you wanted your other sites to route all calls that require gateways to this gatekeeper, you can undo the **lrq reject-unknown-prefix command** by simply using the **no lrq reject-unknown-prefix command.**Now when the gatekeeper receives an LRQ message for the address 12125551234, it attempts to find an appropriate gateway in either one of the zones gk408 or gk415 to service the call.

Related Commands

Command	Description
lrq forward-queries	Enables a gatekeeper to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.

lrq timeout blast window

To configure the timeout window for use when sending multiple location request (LRQ) messages (either sequentially or simultaneously), use the **lrq timeout blast window** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

lrq timeout blast window *seconds*

no lrq timeout blast window

Syntax Description

seconds	Duration of the window, in seconds. Range is from 1 to 10. Default is 6.

Command Default

6 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the window to 3 seconds:

```
lrq timeout blast window 3
```

Related Commands

Command	Description
gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper's zone list.

lrq timeout seq delay

To configure the delay for use when sending location request (LRQ) messages sequentially, use the **lrq timeout seq delay** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

lrq timeout seq delay *value*

no lrq timeout seq delay

Syntax Description

value	Duration of the delay, in 100-millisecond units.Range is from 1 to 10. The default is 5 (500 ms or 0.5 seconds).

Command Default

Five 100-millisecond units (500 ms or 0.5 seconds)

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the window to 300 milliseconds:

```
lrq timeout seq delay 3
```

Related Commands

Command	Description
gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper's zone list.

Cisco IOS Voice Commands: M

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

map q850-cause

To play a customized tone to PSTN callers if a call disconnects with a specific Q.850 call-disconnect cause code and release source, use the **map q850-cause** command in voice-service configuration mode. To disable the code-to-tone mapping, use the **no** form of this command.

map q850-cause *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*

no map q850-cause *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*

Syntax Description

code-id	Q.850 call-disconnect cause code. Range: 1 to 15, 17 to 127 (16 is not allowed).
release-source	Source from which the cause code is generated. Choices are the following: • **local**—Originating gateway or gatekeeper • **remote**—Terminating gateway or gatekeeper • **all**—Any gateway or gatekeeper
tone *tone-id*	Tone to play for this cause code. Choices are the following: • **1**—Busy tone • **2**—Congestion tone • **3**—Special-information tone (a three-tone sequence at 950, 1400, and 1800 MHz) (not supported on IP phones)

Command Default

No mapping occurs.

Command Modes

Voice-service

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to cause a particular tone to play when a call disconnects for a particular reason.

The tone plays to callers only if the call-disconnect and wait-to-release timers are set to values greater than 0 by entering the **timeouts call-disconnect** and **timeouts wait-release** commands.

Examples

The following example maps Q.850 call-disconnect cause code 21 to tone 3 on the local gateway and to tone 2 on the remote gateway:

```
Router(config)# voice service pots
Router(conf-voi-serv)# map q850-cause 21 release-source local tone 3
Router(conf-voi-serv)# map q850-cause 21 release-source remote tone 2
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call setup, progress, or connect messages from an H.323 VoIP gateway.
q850-cause	Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code.
scenario-cause	Configures new Q.850 call-disconnect cause codes for use if an H.323 call fails.
timeouts call-disconnect	Configures the delay timeout before an FXO voice port disconnects an incoming call after disconnect tones are detected.
timeouts wait-release	Configures the delay timeout before the system starts the process for releasing voice ports.

map resp-code

To globally configure a Cisco Unified Border Element (Cisco UBE) to map specific received Session Initiation Protocol (SIP) provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer, use the **map resp-code** command in voice service SIP configuration mode. To disable mapping of received SIP provisional response messages, use the **no** form of this command.

map resp-code 181 to 183

no map resp-code 181

Syntax Description

181	The code representing the specific incoming SIP provisional response messages to be mapped and replaced.
to	The designator for specifying that the specified incoming SIP provisional response message should be mapped to and replaced with a different SIP provisional response message on the outgoing SIP dial peer.
183	The code representing the specific SIP provisional response message on the outgoing dial peer to which incoming SIP message responses should be mapped.

Command Default

Incoming SIP provisional response messages are passed, as is to the outgoing SIP leg.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.

Usage Guidelines

Use the **map resp-code** command in voice service SIP configuration mode to globally enable a Cisco UBE to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outgoing SIP dial peer.

Note If the **block** command is configured for incoming SIP 181 messages, either globally or at the dial-peer level, the messages may be dropped before they can be passed or mapped to a different message—even when the **map resp-code** command is enabled. To globally configure whether and when incoming SIP 181 messages are dropped, use the **block** command in voice service SIP configuration mode (or use the **voice-class sip block** command in dial peer voice configuration mode to configure drop settings on individual dial peers).

To configure mapping of SIP provisional response messages for an individual dial peer on a Cisco UBE, use the **voice-class sip map resp-code** command in dial peer voice configuration mode. To disable mapping of SIP 181 message globally on a Cisco UBE, use the **no map resp-code** command in voice service SIP configuration mode.

As an example, to enable interworking of SIP endpoints that do not support the handling of SIP 181 provisional response messages, you could use the **block** command to configure a Cisco UBE to drop SIP 181 provisional response messages received on the SIP trunk or you can use the **map resp-code** command to configure the Cisco UBE to map the incoming messages to and send out, instead, SIP 183 provisional response messages to the SIP line in Cisco Unified Communications Manager Express (Cisco Unified CME).

Note This command is supported only for SIP-to-SIP calls and will have no effect on H.323-to-SIP or time-division multiplexing (TDM)-to-SIP calls.

Examples

The following example shows how to configure mapping of incoming SIP 181 provisional response messages on the Cisco UBE to SIP 183 provisional response messages on the outbound dial peer:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# map resp-code 181 to 183
```

Related Commands

Command	Description
block	Configures global settings for dropping specific SIP provisional response messages on a Cisco IOS voice gateway or Cisco UBE.
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or Cisco UBE to drop specified SIP provisional response messages.
voice-class sip map resp-code	Configures a specific dial peer on a Cisco UBE to map specific incoming SIP provisional response messages to a different SIP response message.

max1 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address when the suspicion threshold value is reached, use the **max1 lookup** command in MGCP profile configuration mode. To disable lookup, use the **no** form of this command.

max1 lookup

no max1 lookup

Syntax Description This command has no arguments or keywords.

Command Default Lookup is enabled.

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the suspicion threshold. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this number is known as the disconnect threshold. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

Related Commands

Command	Description
call-agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 retries	Sets the MGCP suspicion threshold value.
max2 lookup	Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

max1 retries

To set the Media Gateway Control Protocol (MGCP) suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission), use the **max1 retries** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

max1 retries *number*

no max1 retries

Syntax Description

number	Number of times to attempt to resend messages. Range is from 3 to 30. The default is 5.

Command Default 5 attempts

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced and replaces the **mgcp request retries** command, which is no longer supported.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850 platforms. The maximum number of retries was increased to 30.

Usage Guidelines This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the suspicion threshold. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent.

If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached. This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this is known as the disconnect threshold. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

Related Commands

Command	Description
call-agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached.
max2 lookup	Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max2 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address after the disconnect threshold timeout value is reached, use the **max2 lookup** command in MGCP profile configuration mode. To disable DNS lookup, use the **no** form of this command.

max2 lookup

no max2 lookup

Syntax Description This command has no arguments or keywords.

Command Default Lookup is enabled.

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the *suspicion threshol*d. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this is known as the *disconnect threshold*. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example enables DNS lookup and sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent ca1@exp.example.com
Router(config-mgcp-profile)# max2 lookup
Router(config-mgcp-profile)# max2 retries 9
```

Related Commands

Command	Description
call-agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached.
max1 retries	Sets the MGCP suspicion threshold value.
max2 retries	Sets the MGCP disconnect threshold value.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max2 retries

To set the Media Gateway Control Protocol (MGCP) disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission), use the **max2 retries** command in MGCP profile configuration mode. To disable the disconnect threshold or to return the number of retries to the default, use the **no** form of this command.

max2 retries *number*

no max2 retries

Syntax Description

number	Number of times to attempt to resend messages. Range is from 3 to 30. The default is 7.

Command Default 7 attempts

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced and replaced the **mgcp request retries** command, which is no longer supported.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850. The maximum number of retries was increased to 30.

Usage Guidelines This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the suspicion threshold. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this is known as the disconnect threshold. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

Examples

The following example sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max2 retries 9
```

Related Commands

Command	Description
call-agent	Specifies a call-agent address and protocol for an MGCP profile.
max1 lookup	Enables DNS lookup for an MGCP call agent after the suspicion threshold value is reached.
max1 retries	Sets the MGCP suspicion threshold value.
max2 lookup	Enables DNS lookup for an MGCP call agent after the disconnect threshold value is reached.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

max-calls

To set the maximum number of calls that a trunk group can handle, use the **max-calls** command in trunk group configuration mode. To reset to the default, use the **no** form of this command.

max-calls {**any** | **data** | **voice**} *number* [**direction** [**in** | **out**]]

no max-calls {**any** | **data** | **voice**} *number* [**direction** [**in** | **out**]]

Syntax Description

any	Assigns the maximum number of calls that the trunk group can handle, regardless of the type of call.
data	Assigns the maximum number of data calls to the trunk group.
voice	Assigns the maximum number of voice calls to the trunk group.
number	Range is from 0 to 1000.
direction	(Optional) Specifies direction of calls.
in	(Optional) Allows only incoming calls.
out	(Optional) Allows only outgoing calls.

Command Default

No limit when the command is not set.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to set the maximum number of calls to be handled by the trunk group. If the command is not set the maximum is infinite.

If the maximum is reached, the trunk group becomes unavailable for more calls. When the number of calls falls below the maximum, the trunk group will accept more calls.

Examples

The following example assigns a maximum number of 500 calls of any type to trunk group gw15:

```
Router(config)# trunk group gw15
Router(config-trunk-group)# max-calls any 500
```

The following example assigns a maximum of 200 data calls and 750 voice calls to trunk group 32:

```
Router(config)# trunk group 32
Router(config-trunk-group)# max-calls data 200
Router(config-trunk-group)# max-calls voice 750
```

Related Commands

Command	Description
show trunk group	Displays the configuration of one or more trunk groups.
trunk group	Initiates a trunk group definition.

max-conn (dial peer)

To specify the maximum number of incoming or outgoing connections for a particular Multimedia Mail over IP (MMoIP), plain old telephone service (POTS), Voice over Frame Relay (VoFR), or Voice over IP (VoIP) dial peer, use the **max-conn** command in dial peer configuration mode. To set an unlimited number of connections for this dial peer, use the **no** form of this command.

max-conn *number*

no max-conn

Syntax Description

number	Maximum number of connections for this dial peer. Range is from 1 to 2147483647. Default is an unlimited number of connections.

Command Default

The **no** form of this command is the default, meaning an unlimited number of connections

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to define the maximum number of connections used simultaneously to send or receive fax-mail. This command applies to off-ramp store-and-forward fax functions.

Examples

The following example configures a maximum of 5 connections for VoIP dial peer 10:

```
dial-peer voice 10 voip
 max-conn 5
```

Related Commands

Command	Description
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

max-connection

To set the maximum number of simultaneous connections to be used for communication with a settlement provider, use the **max-connection** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

max-connection *number*

no max-connection *number*

Syntax Description

number	Maximum number of HTTP connections to a settlement provider.

Command Default 10 connections

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples The following command sets the maximum number of simultaneous connections to 10:

```
settlement 0
 max-connection 10
```

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer-id	Sets the customer identification.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the maximum number of connection attempts to the provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
shutdown	Brings up the settlement provider.

Command	Description
type	Configures an SAA-RTR operation type.
url	Configures the ISP address.

max-forwards

To globally set the maximum number of hops, that is, proxy or redirect servers that can forward the Session Initiation Protocol (SIP) request, use the **max-forwards** command in SIP user-agent configuration mode. To reset the default number of hops, use the **no** form of this command.

max-forwards *number-of-hops*

no max-forwards *number-of-hops*

Syntax Description

number-of-hops	Number of hops. Range is from 1 to 70. Default is 70.

Command Default

70 hops

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on Cisco AS5350 and AS5400 platforms.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(8)T	This command was implemented on Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.3(8)T	This command was enhanced with a greater configurable range and a higher default value (compliant with RFC 3261).

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets the number of forwarding requests to 65:

```
sip-ua
 max-forwards 65
```

Related Commands

Command	Description
max-redirects	Sets the maximum number of redirects that the user agent allows.

max-redirects

To set the maximum number of redirect servers that the *n_* allows, use the **max-redirects** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

max-redirects *number*

no max-redirects

Syntax Description

number	Maximum number of redirect servers that a call can traverse. Range is from 1 to 10. The default is 1.

Command Default 1 redirect

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350 platforms.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following is an example of setting the maximum number of redirect servers that the user agent allows:

```
dial-peer voice 102 voip
 max-redirects 2
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.

max-subscription

To set the maximum number of concurrent watch sessions that are allowed, use the **max-subscription** command in presence configuration mode. To return to the default, use the **no** form of this command.

max-subscription *number*

no max-subscription

Syntax Description

number	Maximum watch sessions. Range: 100 to 500. Default: 100.

Command Default

Maximum subscriptions is 100.

Command Modes

Presence (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command sets the maximum number of concurrent presence subscriptions for both internal and external subscribe requests.

Examples

The following example shows the maximum subscriptions set to 150:

```
Router(config)# presence
Router(config-presence)# max-subscription 150
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
presence	Enables presence service on the router and enters presence configuration mode.
presence enable	Allows incoming presence requests from SIP trunks.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

maximum buffer-size

To set the maximum size of the file accounting buffer, use the **maximum buffer-size** command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

maximum buffer-size *kbytes*

no maximum buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range: 6 to 40. Default: 20.

Command Default

Maximum buffer size is 20 kilobytes.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The file accounting process writes call detail records (CDRs) to a memory buffer instead of writing each record independently to the accounting file. Two buffers are allocated for file accounting and their size is set by this command. After the accounting records in the buffer reach the size limit set by this command, the system flushes the first buffer and writes the records to the accounting file. While the first buffer is busy being flushed, the system uses the second buffer to hold new data. After the flush process, the buffer is available again.

The buffer size must be large enough to accommodate incoming CDRs without the system filling up both buffers completely.

Examples

The following example sets the maximum buffer size to 25 kilobytes:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
cdr-format	Selects the format of the CDRs generated for file accounting.
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.

Command	Description
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum cdrflush-timer

To set the maximum time to hold call records in the buffer before appending the records to the accounting file, use the **maximum cdrflush-timer** command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

maximum cdrflush-timer *minutes*

no maximum cdrflush-timer

Syntax Description

minutes	Maximum time, in minutes, to hold call records in the accounting buffer. Range: 1 to 1,435. Default: 60 (1 hour).

Command Default

Records are held in the buffer for 60 minutes (1 hour).

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

After the time period set with this command expires, the router flushes the buffer and writes the call detail records (CDRs) to the accounting file.

The file accounting process sends CDRs to a memory buffer instead of writing each record independently to the accounting file. The system flushes the buffer automatically either after this timer expires or when the records in the buffer reach the size set by the **maximum buffer-size** command.

Set this flush timer to at least five minutes less than the file close timer set with the **maximum fileclose-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

Examples

The following example shows that call records are held in the accounting file for three hours, after which the records are appended to the accounting file:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum conference-participants

To configure the maximum number of conference participants allowed in each meet-me conference, use the **maximum conference-participants** command in DSP farm profile configuration mode. To reset the maximum to the default number, use the **no** form of this command.

maximum conference-participants *max-participants* [**video-cap-class** *number*]

no maximum conference-participants *max-participants* [**video-cap-class** *number*]

Syntax Description

max-participants	Maximum number of participants allowed in each meet-me conference session. One DSP can support the following maximums: • G.711—32 participants • G.729—16 participants • Video (H.263 or H.264)—4, 8, or 16 participants
video-cap-class *number*	(Optional) Reserves the DSP resources needed to support a video participant requiring video format conversion. The range for video port number is from 2 to 4. The default is 2.

Command Default

The default maximum number of participants for a video conference is 4. The default maximum number of participants for an audio conference is 8.

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.1(4)M	This command was modified. The **video-cap-class** keyword was added.

Usage Guidelines

The maximum number of participants allowed for hardware conferencing is dependent on the codec used in the DSP farm profile. Use the **codec** command in DSP farm profile configuration mode to specify the codecs supported by the DSP farm profile. Use the **show dspfarm profile** command to display the DSP farm profile.

Examples

The following example configures a DSP farm profile that has a maximum of 16 participants for hardware conferences using the G.711 codec:

```
Router(config)# dspfarm profile conference 1
Router(config-dspfarm-profile)# maximum conference-participants 16
Router(config-dspfarm-profile)# codec g711alaw
```

Related Commands

Command	Description
codec (DSP Farm profile)	Specifies the codecs supported by a DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions	Specifies the maximum number of sessions that are supported by the profile.
show dspfarm profile	Displays configured DSP farm profile information.

maximum fileclose-timer

To set the maximum time for writing call detail records (CDRs) to an accounting file before closing the file and creating a new one, use the **maximum fileclose-timer** command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

maximum fileclose-timer *minutes*

no maximum fileclose-timer

Syntax Description

minutes	Maximum time, in minutes, to write records to an accounting file. Range: 60 (1 hour) to 1,440 (24 hours). Default: 1,440.

Command Default

Records are saved to an accounting file for 1,440 minutes (24 hours).

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

After the timer set with this command expires, the current accounting file is closed and a new file with a new time stamp is opened to write CDRs. The name and location of the accounting file is set by the **primary** command, or the **secondary** command if in failover mode.

Set this file close timer to at least five minutes longer than the flush timer set with the **maximum cdrflush-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

Examples

The following example shows that call records are saved to the currently open accounting file for 12 hours, after which a new accounting file is created:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum retry-count

To set the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device, use the **maximum retry-count** command in gateway accounting file configuration mode. To reset to the default value, use the **no** form of this command.

maximum retry-count *number*

no maximum retry-count

Syntax Description

number	Number of connection attempts. Range: 1 to 5. Default: 2.

Command Default

Maximum connection attempts is 2.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the number of times that the router attempts to connect to the primary file device defined in the **primary** command before it attempts to connect to the backup file device specified with the **secondary** command.

Examples

The following example shows the maximum retries set to 3:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 cdr-format compact
```

Related Commands

Command	Description
file-acct reset	Manually switches back to the primary device for file-based accounting.
primary	Sets the primary location for storing the call detail records generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

maximum sessions (DSP farm profile)

To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode. To reset to the default, use the **no** form of this command.

Command Syntax When Conferencing or Transcoding Is Configured

maximum sessions *number*

no maximum sessions

Command Syntax When MTP Is Configured

maximum sessions {**hardware** | **software**} *number*

no maximum sessions

Syntax Description

number	Number of session supported by the profile. Range is 0 to *x*. Default is 0. The *x* value is determined at run time depending on the number of resources available with the resource provider.
hardware	Number of sessions that media termination points (MTP) hardware resources will support.
software	Number of sessions that MTP software resources will support.

Command Default

The maximum number of supported sessions is 0.

Command Modes

DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

When using the MTP service type, you must specify the number of sessions separately for software MTP and hardware MTP. The hardware MTP needs digital signal processor (DSP) resources. Use hardware MTP when the codecs are the same and the packetization period is different.

Active profiles must be shut down before any parameters can be changed.

Note The syntax of the command will vary based on the type of profile that you are configuring. The keywords work only when MTP is configured.

Examples

The following example shows that four sessions are supported by the DSP farm profile:

```
Router(config-dspfarm-profile)# maximum sessions
```

Related Commands

Command	Description
associate application	Associates the SCCP protocol to the DSP farm profile.
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
shutdown (dspfarm-profile)	Allocates DSP farm resources and associates with the application.
voice-card	Enters voice-card configuration mode.

mdn

To request that a message disposition notification (MDN) be generated when a message is processed (opened), use the **mdn** command in dial peer configuration mode. To disable generation of an MDN, use the **no** form of this command.

mdn

no mdn

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Message disposition notification is an e-mail message that is generated and sent to the sender when the message is opened by the receiver. Use this command to request that an e-mail response message be sent to the sender when the e-mail that contains the fax TIFF image has been opened.

This command applies to on-ramp store-and-forward fax functions.

Examples The following example requests that a message disposition notification be generated by the recipient:

```
dial-peer voice 10 mmoip
 mdn
```

Related Commands

Command	Description
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta send return-receipt-to	Specifies the address to which MDNs are sent.

media

To enable media packets to pass directly between the endpoints, without the intervention of the Cisco Unified Border Element (Cisco UBE) and to enable signaling services, enter the **media** command in dial peer voice, voice class, or voice service configuration mode. To return to the default behavior, use the **no** form of this command.

media [**flow-around | flow-through | forking | monitoring** [*max-calls*] **| statistics | transcoder high-density | anti-trombone | sync-streams**]

no media [**flow-around | flow-through | forking | monitoring** [*max-calls*] **| statistics | transcoder high-density | anti-trombone | sync-streams**]

Syntax Description

flow-around	(Optional) Enables media packets to pass directly between the endpoints, without the intervention of the Cisco UBE. The media packet is to flow around the gateway.
flow-through	(Optional) Enables media packets to pass through the endpoints, without the intervention of the Cisco UBE.
forking	(Optional) Enables the media forking feature for all calls.
monitoring	(Optional) Enables the monitoring feature for all calls or a maximum number of calls.
max-calls	(Optional) The maximum number of calls that are monitored.
statistics	(Optional) Enables media monitoring.
transcoder high-density	(Optional) Converts media codecs from one voice standard to another to facilitate the interoperability of devices using different media standards.
anti-trombone	(Optional) Enables media anti-trombone for all calls. Media trombones are media loops in SIP entity due to call transfer or call forward.
sync-streams	(Optional) Specifies that both audio and video streams go through the DSP farms on Cisco UBE and Cisco Unified CME.

Command Default

The default behavior of the Cisco UBE is to receive media packets from the inbound call leg, terminate them, and then reoriginate the media stream on an outbound call leg.

Command Modes

Dial peer voice configuration (config-dial-peer)
Voice class configuration (config-class)
Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)T	This command was introduced.
12.4(11)XJ2	This command was modified. The **statistics** keyword was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(20)T	This command was modified. The **transcoder** and **high-density** keywords were introduced.

Release	Modification
15.0(1)M	This command was modified. The **forking** and **monitoring** keywords and the *max-calls* argument were introduced.
15.1(3)T	This command was modified. The **anti-trombone** keyword was introduced.
15.1(4)M	This command was modified. The **sync-stream** keyword was added.

Usage Guidelines

With the default configuration, the Cisco UBE receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco UBE. The Cisco UBE continues to handle routing and billing functions. Media flow-around for SIP-to-SIP calls is not supported.

Note The Cisco UBE must be running Cisco IOS Release 12.3(1) or a later release to support media flow-around.

You can specify media flow-around for a voice class, all VoIP calls, or individual dial peers.

The **transcoder high-density** keyword can be enabled in any of the configuration modes with the same command format. If you are configuring the **transcoder high-density** keyword for dial peers, make sure that the **media transcoder high-density** command is configured on both the in and Out-Legs.

Note The software does not support configuring the **transcoder high-density** keyword on any dial peer that is to handle video calls. The following scenarios are not supported:

- Dial peers used for video at any time. Configuring the **media transcoder high-density** command directly under the dial-peer or a voice-class media configuration mode is not supported.
- Dial peers configured on a Cisco UBE used for video calls at any time. The global configuration of the **media transcoder high-density** command under voice service configuration mode is not supported.

To enable the **media** command on a Cisco 2900 or Cisco 3900 series Unified Border Element voice gateway, you must first enter the **mode border-element** command. This enables the **media forking** and **media monitoring** commands. Do not configure the **mode border-element** command on the Cisco 2800 or Cisco 3800 series platform.

You can specify media anti-trombone for a voice class, all VoIP calls, or individual dial peers.

The **anti-trombone** keyword can be enabled only when no media interworking is required in both the Out-Legs. Antitrombone will not work if call leg is flow-through and another call leg is flow-around.

Examples

Media Flow-around Examples

The following example shows media flow-around configured on a dial peer:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# media flow-around
```

The following example shows media flow-around configured for all VoIP calls:

```
Router(config)# voice service voip
Router(config-voi-serv)# media flow-around
```

The following example shows media flow-around configured for voice class calls:

```
Router(config)# voice class media 1
Router(config-class)# media flow-around
```

Media Flow-through Examples

The following example shows media flow-through configured on a dial peer:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# media flow-through
```

The following example shows media flow-through configured for all VoIP calls:

```
Router(config)# voice service voip
Router(config-voi-serv)# media flow-through
```

The following example shows media flow-through configured for voice class calls:

```
Router(config)# voice class media 2
Router(config-class)# media flow-through
```

Media Statistics Examples

The following example shows media monitoring configured for all VoIP calls:

```
Router(config)# voice service voip
Router(config-voi-serv) media statistics
```

The following example shows media monitoring configured for voice class calls:

```
Router(config)# voice class media 1
Router(config-class) media statistics
```

Media Transcoder High-density Examples

The following example shows the **media transcoder** command configured for all VoIP calls:

```
Router(config)# voice service voip
Router(conf-voi-serv)# media transcoder high-density
```

The following example shows the **media transcoder** command configured for voice class calls:

```
Router(config)# voice class media 1
Router(config-voice-class)# media transcoder high-density
```

The following example shows the **media transcoder** command configured on a dial peer:

```
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# media transcoder high-density
```

Media Monitoring on a Cisco UBE Platform

The following example shows how to configure audio call scoring for a maximum of 100 calls:

```
mode border-element
media monitoring 100
```

Media Antitrombone Examples

The following example shows the **media anti-trombone** command configured for all VoIP calls:

```
Router(config)# voice service voip
Router(conf-voi-serv)# media anti-trombone
```

The following example shows the **media anti-trombone** command configured for voice class calls:

```
Router(config)# voice class media 1
Router(config-voice-class)# media anti-trombone
```

The following example shows the **media anti-trombone** command configured on a dial peer:

```
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# media anti-trombone
```

Media Transcoder Examples

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed:

```
Router(config)# voice service voip
Router(config-voi-serv)# media transcoder sync-streams
```

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed and the RTP streams flow around Cisco Unified Border Element.

```
Router(config)# voice service voip
Router(config-voi-serv)# media transcoder high-density sync-streams
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer voice configuration mode.
mode border-element	Enables the media monitoring capability of the **media** command.
voice class	Enters voice class configuration mode.
voice service	Enters voice service configuration mode.

mediacard

To enter mediacard configuration mode and configure a Communications Media Module (CMM) media card, use the **mediacard** command in global configuration mode.

mediacard *slot*

Syntax Description

slot	Specifies the slot number for the media card to be configured. Valid values are from 1 to 4.

Command Default

No default behavior or values

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Mediacard configuration mode is used to configure parameters related to the selected media card, such as digital signal processor (DSP) resource pools.

Examples

The following example shows how you configure DSP resources on the media card in slot 1:

```
mediacard 1
```

Related Commands

Command	Description
debug mediacard	Displays debugging information for Digital Signal Processor Resource Manager (DSPRM).
show mediacard	Displays information about the selected media card.

media-inactivity-criteria

To specify the mechanism for detecting media inactivity (silence) on a voice call, use the **media-inactivity-criteria** command in gateway configuration mode. To disable detection, use the **no** form of this command.

media-inactivity-criteria {**rtp** | **rtcp** | **all**}

no media-inactivity-criteria

Syntax Description

rtp	Real-Time Transport Protocol (RTP) (default)
rtcp	RTP Control Protocol (RTCP)
all	Both RTP and RTCP

Command Default

Media-inactivity detection is performed by means of RTP.

Command Modes

Gateway

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to specify the mechanism for detecting silence on a voice call. After doing so, you can configure silent calls to disconnect by entering the related commands listed below.

Use this command, in conjunction with the **application**, **package callfeature**, **param**, and **paramspace** commands, to configure callfeature parameters at the package level and to override them as needed for specific applications or dial peers.

The mechanism that you explicitly specify with this command takes precedence over any mechanism that you might implicitly have specified with the **ip rtcp report interval** command in combination with the **timer media-inactive** or **timer receive-rtcp** command.

Examples

The following example specifies the use of RTCP for silence detection:

```
Router(config)# gateway
Router(config-gateway)# media-inactivity-criteria rtcp
```

The following example shows a configuration that might result from the use of this and related commands:

```
voice service pots
map q850-cause 44 release-source local tone 3

application
 package callfeature
  param med-inact-disc-cause 44
  param med-inact-det enable
  param med-inact-action disconnect
ip rtcp report interval 9000
dial-peer voice 5 voip
destination-pattern .T
 progress_ind disconnect enable 8
 session target ras
 codec g711ulaw
gateway
 media-inactivity-criteria rtcp
 timer media-inactive 5
```

Related Commands

Command	Description
application	Enables a specific application on a dial peer.
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.
package callfeature	Enters application-parameter configuration mode.
param	Loads and configures parameters in a package or a service (application) on the gateway.
paramspace	Enables an application to use parameters from the local parameter space of another application.
timer media-inactive	Sets the media-inactivity disconnect timer.
timer receive-rtcp	Sets the RTCP timer and configures a multiplication factor for the RTCP timer interval for SIP or H.323 calls.

meetme-conference

To define a feature code for a Feature Access Code (FAC) to initiate an SCCP Meet-Me Conference, use the **meetme-conference** command in STC application feature access-code configuration mode. To return the feature code to its default, use the **no** form of this command.

meetme-conference *keypad-character*

no meetme-conference

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 5. The string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default The default value of the feature code is 5.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for SCCP Meet-Me Conference from the default (5) to the specified value.

If the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 55#, the phone user dials only 55#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

If you attempt to configure this command with a value that is already configured for another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

If you attempt to configure this command with a value that precludes or is precluded by another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for SCCP Meet-Me Conference from the default (5). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##9 on the phone keypad to cancel all-call forwarding.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# meetme-conference 9
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

member (dial peer cor list)

To add a member to a dial peer class of restrictions (COR) list, use the **member** command in dial peer COR list configuration mode. To remove a member from a list, use the **no** form of this command.

member *class-name*

no member *class-name*

Syntax Description

class-name	Class name previously defined in dial peer COR custom configuration mode by using of the **name** command.

Command Default No default behavior or values.

Command Modes Dial peer COR list configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples The following example adds three members to the COR list named list3:

```
dial-peer cor list list3
 member 900_call
 member 800_call
 member catchall
```

Related Commands

Command	Description
dial-peer cor list	Defines a COR list name.

method

To set a specific accounting method list, use the **method** command in gateway accounting AAA configuration mode.

method *acctMethListName*

Syntax Description

acctMethListName	Name of the accounting method list.

Command Default

H.323 is the default accounting method list.

Command Modes

Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- For information on setting AAA network security for your network, including setting method lists, refer to the *Authentication, Authorization, and Accounting Cisco IOS Security Configuration Guide, Release 12.2*.
- The **method** command sets the accounting method globally (not for a dial peer). To initially define the AAA method list name for accounting, use the **aaa accounting** command.
- The method list name used is the same name used to define the method list name under the **aaa accounting** command.

Examples

The following example uses the method list named “klz_aaa6” that was previously defined using the AAA commands.

```
aaa new-model
!
aaa group server radius sg6
server 1.6.30.70 auth-port 1708 acct-port 1709
!
aaa authentication login klz_aaa6 group sg6
! klz_aaa6 is defined as the method list name.
aaa authorization exec klz_aaa6 group sg6
aaa accounting connection klz_aaa6 start-stop group sg6
!
gw-accounting aaa
method klz_aaa6
! The same method list named klz_aaa6 is used.
```

Related Commands

Command	Description
aaa accounting	Enables accounting of requested services for billing or security purposes.
gw-accounting aaa	Enables VoIP gateway accounting.

mgcp

To allocate resources for the Media Gateway Control Protocol (MGCP) and start the MGCP daemon, use the **mgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and stop the MGCP daemon, use the **no** form of this command.

mgcp [*port*]

no mgcp

Syntax Description

port	(Optional) User Datagram Protocol (UDP) port for the MGCP gateway. Range is from 1025 to 65535. The default is UDP port 2427.

Command Default UDP port 2427

Command Modes Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 3660, Cisco uBR924, and Cisco 2600 series.
12.1(5)XM	This command was added to Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines Once you start the MGCP daemon using the **mgcp** command, you can suspend it (for example, for maintenance) by using the **mgcp block-newcalls** command. When you are ready to resume normal MGCP operations, use the **no mgcp block-newcalls** command. Use the **no mgcp** command only if you intend to terminate all MGCP applications and protocols.

When the MGCP daemon is not active, all MGCP messages are ignored.

If you want to change the UDP port while MGCP is running, you must stop the MGCP daemon using the **no mgcp** command, and then restart it with the new port number using the **mgcp** *port* command.

Examples The following example initiates the MGCP daemon:

```
Router(config)# mgcp
```

The following example enables the MGCP daemon on port 4204:

```
Router(config)# mgcp 4204
```

Related Commands

Command	Description
application	Enables debugging on MGCP.
debug mgcp	Enables debugging on MGCP.
mgcp block-newcalls	Gracefully terminates all MGCP activity.
mgcp ip-tos	Enables or disables the IP ToS for MGCP connections.
mgcp request retries	Specifies the number of times to retry sending the **mgcp** command.
show mgcp	Displays the MGCP parameter settings.

mgcp behavior

To configure a gateway to alter the Media Gateway Control Protocol (MGCP) behavior, use the **mgcp behavior** command in global configuration mode. To resume using the standard protocol version behavior that is specified in the configuration, use the **no** form of this command.

mgcp behavior *category version*

no mgcp behavior *category version*

Syntax Description

category	MGCP behavior category. For valid values, see Table 33.
version	MGCP version for the behavior category. For valid values, see Table 34.

Command Default

The gateway follows the rules and guidelines that are specified by the configured MGCP protocol version.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T1	This command was introduced.
12.3(4)T	This command was modified. The **signals v0.1** keyword was added.
12.3(8)T	This command was modified. The **dlcx-clear-signals** keyword was added.
12.3(11)T	This command was modified. The **ack-init-rsip disable** and **init-rsip-per-insvc legacy** keywords were added.
12.3(14)T	This command was modified. The **q-mode-enduring legacy** keyword was added.
12.3(16)	This command was modified. The **mdcx-sdp ack-with-sdp** keyword was added.
12.4(4)T	This command was modified. The **rsip-range** keyword was added.
12.4(24)T	This command was modified. The default behavor of the mode parameter in the SDP was given higher preference to the mode present in the M: line of the MGCP message. The **digit-collect-stuck play-reorder**, **fxs-gs emulate-ls-disconnect**, **mode-attrb-in-sdp disable,** **private-localhost**, and **transient-state-response enable** keywords were added.
15.1(1)T	This command was modified. The **dynamically-change-codec-pt disable** keyword was added.
15.1(3)T	This command was modified. The **negotiate-nse enable** keyword was added.

Usage Guidelines

Table 33 describes the MGCP behavior category keywords.

Table 33 MGCP Behavior Category Keywords

Keywords	Description
ack-init-rsip disable	Forces the gateway to accept commands from the call agent before its initial ReStart In Progress (RSIP) messages are acknowledged; that is, 405 error codes do not occur. The gateway also behaves in this way if it is configured for MGCP Version 1.0 and earlier versions. By default, or when the **no** form of this command is issued, if the gateway is configured for MGCP Version RFC 3435-1.0 or later versions, it responds to call agent commands with a 405 error code until its initial RSIPs are acknowledged by the call agent.
digit-collect-stuck play-reorder	Forces the gateway to play a reorder tone to the user when 60 seconds have passed and when MGCP is in the process of collecting the digits. By default, or when the **no** form of this command is issued, if the MGCP application does not get a connection or gets disconnected within a specific time when the endpoint is in the off-hook state, then the endpoint may be busy in the digit collection state.
dlcx-clear-signals all	Forces the gateway to turn off or clear all signals when it receives a Delete Connection (DLCX) message from the call agent even if there is no S: line in the message. By default, and as specified by RFC 3435, the gateway maintains current endpoint signals if a DLCX has no S: line. The MGCP gateway clears signals only when the call agent explicitly turns off each signal or sends an empty S: line to clear all signals.
dynamically-change-codec-pt disable	Forces the gateway not to change the codec payload type when it is dynamically changed in the incoming Session Description Protocol (SDP). By default, or when **no** form of this command is issued, MGCP dynamically changes the payload, if the incoming SDP has a different codec.
fxs-gs emulate-ls-disconnect	Forces the gateway not to disconnect the call even when the gateway receives a DLCX for a ground-start enabled endpoint. The gateway plays the busy tone as the call does not get disconnected. By default, or when **no** form of this command is issued, MGCP disconnects the call when it receives a DLCX.

Table 33 MGCP Behavior Category Keywords (continued)

Keywords	Description
init-rsip-per-insvc legacy	Forces the gateway to always use the restart method of Restart for its initial RSIP messages, regardless of the service state of the endpoints. Wildcard demotion may occur as needed, based on configuration. By default, or when the **no** form of this command is issued, if the MGCP gateway is running Version RFC 3435-1.0, the default restart method for initial RSIPs depends on the service state of the endpoint. For in-service endpoints, the restart method is Restart. For out-of-service endpoints, the restart method is Forced. Additionally, regardless of the protocol version, the gateway always attempts to use a wildcard RSIP * message to minimize the number of messages that are sent to the call agent. The gateway sends the fully wildcarded RSIP * message as long as the following requirements are met: • MGCP is configured for a single profile (or the default profile) only. • A single DS0 group is configured for each DS1. • The single DS0 group includes all the possible DS0s. • All endpoints are in the same service state (when the MGCP call agent is configured for Version RFC 3435-1.0 and the **no** form of this command is issued). If any one of these requirements is not met, the initial RSIP * message is demoted and sent as multiple RSIP messages to the call agent. When demoting, the gateway continues to attempt to minimize the number of RSIP messages.
mdcx-sdp ack-with-sdp	Forces the gateway to generate a SDP in response to a modify connection (MDCX) message that contains an SDP. The response contains the SDP only if the MDCX is responded to with a positive (200) acknowledgment. By default, or when the **no** form of this command is issued, the positive acknowledgment reply generates an SDP only if any of the parameters have changed from the previous SDP that was generated by the gateway. With this command, even if all the parameters are the same as the previous SDP, the SDP is still generated. This enables operation with a SIP gateway that expects an SDP response to every CRCX or MDCX message.
mode-attrb-in-sdp disable	Forces the gateway to take connection mode M in Create Connection (CRCX). By default, or when **no** form of this command is issued, preference is given to the connection mode present in SDP. This is only when the mode is present in SDP.
negotiate-nse enable	Makes MGCP gateway aware of the remote side's Named Signaling Event (NSE) capabilities by examining the remote SDP for NSE capabilities. By default, or when the **no** form of this command is issued, NSE is disabled on the gateway. Cisco Unified Call Manager (UCM) does not support modem or fax passthrough. This feature should not be enabled when Cisco UCM is the call agent.

Table 33 MGCP Behavior Category Keywords (continued)

Keywords	Description
private-localhost	Requires the outgoing messages from the gateway, like Notify (NTFY), RSIP, DLCX, have the private-localhost appended to the endpoint ID. By default, or when the **no** form of this command is issued, the outgoing messages from the gateway have the global router name appended to the endpoint ID. This is applicable for MGCP 0.1 and MGCP 1.0 versions.
q-mode-enduring legacy	Allows the gateway to keep the current quarantine mode when a request notification (RQNT) does not contain a Q: line. Operation reverts to legacy behavior, which is the following: **Note** Only the first bulleted item results in modified behavior. • No Q: line—Makes no changes to the quarantine mode (whatever mode was set in the previous command persists). • Empty Q: line—Resets the quarantine mode to the default. • Valid Q: line—Sets the quarantine mode per command. • Invalid Q: line—Generates an error. **Note** The quarantine mode is set with the **mgcp quarantine mode** command, and the default is discarded. This is the configuration mode used if the quarantine mode is not specified in the RQNT or embedded request for events. By default, or when the **no** form of this command is issued, MGCP behaves according to both MGCP Version 0.1 and MGCP Version 1.0 specifications—that is, the MGCP gateway resets the quarantine mode to the default in the running configuration if no Q: line is present.
rsip-range	Determines whether the gateway can generate RSIP messages with endpoint ranges for versions other than Trunking Gateway Control Protocol (TGCP). By default, endpoint ranges are generated in RSIP messages for TGCP only. The following *category* and *version* values can be configured: • **rsip-range all**—Allows the gateway to generate endpoint ranges in RSIP messages for all MGCP versions. • **rsip-range none**—Prevents the gateway from generating endpoint ranges for all MGCP versions, including TGCP. • **rsip-range tgcp-only**—Allows the gateway to generate endpoint ranges in RSIP messages only if the configured protocol is TGCP. This is the default value. TGCP specifications require support for endpoint ranges in RSIP messages. Not all call agents may support this functionality however. In such cases, selecting **none** allows the gateway to interoperate with these call agents. Conversely, if a non-TGCP call agent supports endpoint ranges, selecting **all** allows the gateway to take advantage of this functionality.

Table 33 MGCP Behavior Category Keywords (continued)

Keywords	Description
transient-state-response enable	Forces the gateway to send 400 responses for an MGCP message even if the endpoint is in a transient state. By default, or when **no** form of this command is issued, the gateway does not respond to MGCP messages even if the endpoint is in a transient or disconnecting state.

Table 34 describes the MGCP behavior version keywords.

Table 34 MGCP Behavior Version Keywords

Keywords	Description
auep v0.1	Forces the gateway to reply to an Audit Endpoint (AUEP) command according to the MGCP Version 0.1 specification. This behavior applies specifically to the case in which the endpoint being audited is out of service. If this command is used, an AUEP command on an out-of-service endpoint returns error code of 501. By default, or when the **no** form of this command is issued, MGCP Version 1.0 behavior occurs—that is, response code 200 is sent for all valid endpoints, regardless of their service state, and requested audit information follows. In either case, the configured MGCP version is ignored.
signals v0.1	Forces the gateway to handle call signaling tones such as ringback, network congestion, reorder, busy, and off-hook warning tones according to the MGCP Version 0.1 specification. The MGCP Version 0.1 specification treats some call signaling tones as on-off tones, which terminate only after a specific MGCP message has been received to stop the signal. By default, or when the **no** form of this command is issued, RFC 3660 is followed, which treats the call signaling tones as timeout tones that terminate when the appropriate timeout expires. In either case, the configured MGCP version is ignored.

Examples

The following example shows how the gateway sends MGCP 0.1 responses to AUEP commands:

```
Router(config)# mgcp behavior auep v0.1
```

The following example shows how the gateway provides MGCP 0.1 treatment of call signaling tones:

```
Router(config)# mgcp behavior signals v0.1
```

The following example shows how to disable the requirement that the RSIP be acknowledged before a call agent command is accepted:

```
Router(config)# mgcp behavior ack-init-rsip disable
```

The following example show how to configure the gateway to not demote initial RSIPs based on the service state of the endpoints:

```
Router(config)# mgcp behavior init-rsip-per-insvc legacy
```

The following example shows how to configure the gateway to turn off all signals on receipt of a DLCX:

```
Router(config)# mgcp behavior dlcx-clear-signals all
```

The following examples show how to set quarantine mode to legacy:

```
Router(config)# mgcp behavior q-mode-enduring legacy
```

The following example shows how to force the gateway to generate an SDP in the response to an MDCX with SDP:

```
Router(config)# mgcp behavior mdcx-sdp ack-with-sdp
```

The following example shows how to force the gateway to generate endpoint ranges for all MGCP versions:

```
Router(config)# mgcp behavior rsip-range all
```

The following example shows how to force the gateway not to change the codec payload type when it is dynamically changed in the incoming SDP for all MGCP versions:

```
Router(config)# mgcp behavior dynamically-change-codec-pt disable
```

The following example shows how to force the gateway not to disconnect when it receives DLCX:

```
Router(config)# mgcp behavior fxs-gs emulate-ls-disconnect
```

The following example shows how forces the gateway to send responses for MGCP messages even if the endpoint is in a transient state:

```
Router(config)# mgcp behavior transient-state-response enable
```

The following example shows how to force the gateway to take connection mode M in CRCX:

```
Router(config)# mgcp behavior mode-attrb-in-sdp disable
```

The following example shows how to force the outgoing messages to have the configured private–localhost appended to the endpoint ID for MGCP 0.1 and MGCP 1.0 versions:

```
Router(config)# mgcp behavior private-localhost cisco.com
```

The following example shows how to force the gateway to play a reorder tone when MGCP is still stuck trying to collect digits:

```
Router(config)# mgcp behavior digit-collect-stuck play-reorder
```

The following example shows how to allow the gateway to be aware of NSE capabilities:

```
Router(config)# mccp behavior negotiate-nse enable
```

Use the following commands to display the MGCP behavior and versions settings:

```
Router# show running-config | include behavior

mgcp behavior auep v0.1
mgcp behavior signals v0.1
mgcp behavior ack-init-rsip disable
mgcp behavior init-rsip-per-insvc legacy
mgcp behavior q_mode-enduring legacy
mgcp behavior dlcx-clear-signals all
mgcp behavior mdcx-sdp ack-with-sdp
mgcp behavior rsip-range all
mgcp behaviour dynamically-change-codec-pt disable
mgcp behavior fxs-gs emulate-ls-disconnect
mgcp behavior transient-state-response enable
mgcp behavior mode-attrb-in-sdp-disable
```

```
mgcp behavior private-localhost cisco.com
mgcp behavior digit-collect-stuck- play-reorder
mgcp behavior negotiate-nse enable

Router# show running-config | include call-agent

mgcp call-agent ca123.example.net 4040 service-type mgcp version rfc3435-1.0
```

Related Commands

Command	Description
mgcp	Allocates resources for MGCP and starts the MGCP daemon.
mgcp call-agent	Specifies the address and protocol for the MGCP call agent.
mgcp quarantine mode	Configures the mode for MGCP quarantined events.
show mgcp	Displays values for MGCP parameters.
show running-config	Displays the contents of the currently running configuration file.

mgcp behavior comedia-check-media-src

To force IP address and port detection from the first RTP packet received for the entire Media Gateway Control Protocol (MGCP) gateway and enable the callback function selected by MGCP, use the **mgcp behavior comedia-check-media-src** command in global configuration mode.

mgcp behavior comedia-check-media-src {**enable** | **disable**}

Syntax Description

enable	Forces ip address and port detection.
disable	Disables ip address and port detection.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use the **mgcp behavior comedia-check-media-src** command to force IP address and port detection from the first rtp packet received for the entire MGCP gateway. This command also enables the callback function selected by MGCP, and with the configuration of the **mgcp behavior comedia-role** command contributes to the determination of whether to populate the SDP direction attribute.

Examples The following example shows IP address and port detection being enabled for the entire MGCP gateway:

```
Router(config)# mgcp behavior comedia-check-media-src enable
```

Related Commands

Field	Description
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-role	Specifies the location of the configured MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior comedia-role

To specify the location of the configured Media Gateway Control Protocol (MGCP) gateway, use the **mgcp behavior comedia-role** command in global configuration mode.

mgcp behavior comedia-role {**active** | **passive** | **none**}

Syntax Description

active	Specifies MGCP gateways located inside NAT.
passive	Specifies MGCP gateways located outside of NAT.
none	Specifies gateway behavior be as in releases prior to Cisco IOS Release 12.4(11)T.

Command Default

none

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command will specify the location of the configured MGCP gateway and its role in solving the NAT media traversal. A comedia role of **active** is configured for MGCP gateways inside NAT. For gateways located outside of NAT a comedia role of **passive** is configured. Configuring the **none** keyword specifies gateway behavior before the **mgcp behavior comedia-role** command was introduced.

The **mgcp behavior comedia-role** and **mgcp behavior comedia-check-media-src** commands are used to determine when to populate the sdp direction attribute.

Examples

The following example shows the location of the MGCP gateway configured for MGCP gateways inside NAT:

```
Router(config)# mgcp behavior comedia-role active
```

Related Commands

Field	Description
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
mgcp	Allocates resources for the MGCP and starts the daemon.
show mgcp	Displays the entire mgcp configuration.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior comedia-sdp-force

To force MGCP to place the direction attribute in the Session Description Protocol (SDP), use the **mgcp behavior comedia-sdp-force** command in global configuration mode.

mgcp behavior comedia-sdp-force {**enable** | **disable**}

Syntax Description

enable	Forces MGCP to place the direction attribute in the SDP.
disable	Allows the **mgcp behavior comedia-role**, and **mgcp behavior comedia-check-media-src** commands and the remote descriptor to determine if the direction attribute is added to the SDP.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command will force the MGCP to always place the direction attribute in the SDP using the **mgcp behavior comedia-sdp-force** command as a reference. When the **mgcp behavior comedia-sdp-force** command is configured with the **disable** keyword, the **mgcp behavior comedia-role** and **mgcp behavior comedia-check-media-src** commands and the remote descriptor determine if the direction is added to the SDP. If the role is not configured, this command has no effect.

Examples

The following example configuration forces the direction attribute to be placed in the SDP:

```
Router(config)# mgcp behavior comedia-sdp-force enable
```

Related Commands

Field	Description
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Specifies the location of the configured MGCP gateway.
show mgcp connection	Displays information for active MGCP-controlled connections.

mgcp behavior g729-variants static-pt

To change the default from dynamic to static Real-time Transport Protocol (RTP) payload type on G.729 voice codecs, use the **mgcp behavior g729-variants static-pt** command in global configuration mode. To return the default to dynamic, use the **no** form of this command.

mgcp behavior g729-variants static-pt

no mgcp behavior g729-variants static-pt

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default, so the RTP payload type on G.729 voice codecs is static.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T2 12.4(24)T1	This command was modified to be enabled by default.

Usage Guidelines

Prior to Cisco IOS Releases 12.4(22)T2 and 12.4(24)T1, the negotiated value (dynamic) payload type was not set in RTP packets. If you upgraded the Cisco IOS software on your network voice gateways (with existing Cisco Unified Communications Manager) and calls were going between Skinny Client Control Protocol (SCCP) phones controlled by Cisco Unified Communications Manager and public switched telephone network (PSTN) phones connected to a Cisco gateway, a condition of “no audio” could occur. The **mgcp behavior g729-variants static-pt** command changes the default from dynamic to static RTP payload type on G.729 voice codecs and eliminates the “no audio” condition.

Examples

The following example shows how to set the RTP payload type to static for G.729 voice codecs:

```
Router(config)# mgcp behavior g729-variants static-pt
```

Related Commands

Command	Description
mgcp codec	Selects the default codec type and its optional packetization period value.
mgcp rtp payload-type	Specifies use of the correct RTP payload type for backward compatibility in MGCP networks.

mgcp bind

To configure the source address for signaling and media packets to the IP address of a specific interface, use the **mgcp bind** command in global configuration mode. To disable binding, use the **no** form of this command.

mgcp bind {**control** | **media**} **source-interface** *interface-id*

no mgcp bind {**control** | **media**}

Syntax Description

control	Binds only Media Gateway Control Protocol (MGCP) control packets.
media	Binds only media packets.
source-interface	Specifies an interface as the source address of MGCP or Session Initiation Protocol (SIP) packets. **Note** The MGCP Gateway Support for the mgcp bind Command feature does not support SIP.
interface-id	Specifies the interface for source address of MGCP packets. The following are valid source addresses: • **Async**—Async interface • **BVI**—Bridge-Group Virtual Interface • **CTunnel**—CTunnel interface • **Dialer**—Dialer interface • **FastEthernet**—Fast Ethernet IEEE 802.3 • **Lex**—Lex interface • **Loopback**—Loopback interface • **MFR**—Multilink Frame Relay bundle interface • **Multilink**—Multilink-group interface • **Null**—Null interface • **Serial**—Serial • **Tunnel**—Tunnel interface • **Vif**—PGM Multicast Host interface • **Virtual-Template**—Virtual Template interface • **Virtual-TokenRin**g—Virtual Token Ring

Command Default Binding is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced for MGCP on the Cisco 2400 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco IAD2421, Cisco MC3810, and Cisco VG200.

Usage Guidelines

If the **mgcp bind** command is not enabled, the IP layer still provides the best local address.

A warning message is displayed if any of the following situations occur:

- When there are active MGCP calls on the gateway, the **mgcp bind** command is rejected for both control and media.
- If the bind interface is not up, the command is accepted but does not take effect until the interface comes up.
- If the IP address is not assigned on the bind interface, the **mgcp bind** command is accepted but takes effect only after a valid IP address is assigned. During this time, if MGCP calls are up, the **mgcp bind** command is rejected.
- When the bound interface goes down, either because of a manual shutdown on the interface or because of operational failure, the bind activity is disabled on that interface.
- When bind is not configured on the media gateway controller (MGC), the IP address used for sourcing MGCP control and media is the best available IP address.

Examples

The following example shows how the configuration of bind interfaces is shown when **show running-config** information is viewed:

```
.
.
.
mgcp bind control source-interface FastEthernet0
mgcp bind media source-interface FastEthernet0
.
.
.
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp block-newcalls

To block new calls while maintaining existing calls, use the **mgcp block-newcalls** command in global configuration mode. To resume media gateway control protocol (MGCP) operation, use the **no** form of this command.

mgcp block-newcalls

no mgcp block-newcalls

Syntax Description

This command has no arguments or keywords.

Command Default

New call are not blocked.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

This command is valid only if the **mgcp** command is enabled.

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until participants terminate them or you use the **no mgcp** command. When the last active call is terminated, the MGCP daemon is terminated and all resources that are allocated to it are released. The **no mgcp block-newcalls** command returns the router to normal MGCP operations.

Examples

The following example prevents the gateway from receiving new calls:

```
Router(config)# mgcp block-newcalls
```

Related Commands

Command	Description
mgcp	Allocates resources for the MGCP and starts the daemon.

mgcp call-agent

To configure the address and protocol of the call agent for Media Gateway Control Protocol (MGCP) endpoints on a media gateway, use the **mgcp call-agent** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp call-agent {*host-name* | *ip-address*} [*port*] [**service-type** *type* [**version** *protocol-version*]]

no mgcp call-agent

Syntax Description

host-name	Fully qualified domain name (including host portion) for the call agent; for example, ca123.example.net.
ip-address	IP address for the call agent.
port	(Optional) User Datagram Protocol (UDP) port over which the gateway sends messages to the call agent. Range is from 1025 to 65535.
service-type *type*	(Optional) Type of Gateway control service protocol. It can be one of the following values: • **mgcp**—Media Gateway Control Protocol • **ncs**—Network Communication Server • **sgcp**—Simple Gateway Control Protocol • **tgcp**—Trunking Gateway Control Protocol
version *protocol-version*	(Optional) Version of gateway control service protocol. It can be one of the following values: • For **service-type mgcp**: 0.1, 1.0, rfc3435-1.0 – 0.1—Version 0.1 of MGCP (Internet Draft) – 1.0—Version 1.0 of MGCP (RFC2705 Version 1.0) – rfc3435-1.0—Version 1.0 of MGCP (RFC3435 Version 1.0) **Note** This configuration value is used to allow the router to tailor the MGCP application behavior to be compatible based on the RFC2705 or RFC3435 definitions. • For **service-type ncs**: 1.0 • For **service-type sgcp**: 1.1, 1.5 • For **service-type tgcp**: 1.0

Command Default

Call-agent UDP port: 2727 for MGCP 1.0, NCS 1.0, and TGCP 1.0
Call-agent UDP port: 2427 for MGCP 0.1 and SGCP
Call-agent UDP port: 2427 for Cisco CallManager
Service type and version: mgcp 0.1
Service type for Cisco CallManager: mgcp

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	The **service-type** *type* keyword and argument were added.
12.1(5)XM	The **version** *protocol-version* keyword and argument were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	New service types (**ncs** and **tgcp**) and appropriate versions were added. Version 1.0 was added for the **mgcp** service type. This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XN	This command was implemented to provide enhanced MGCP voice gateway interoperability on Cisco CallManager Version 3.1 for the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.3(8)T 1	This command was modified by adding the RFC3435-1.0 option to the command.

Usage Guidelines

Global call-agent configuration (with this command) and call-agent configuration for an MGCP profile (with the **mgcp profile call-agent** command) are mutually exclusive; the first to be configured on an endpoint blocks configuration of the other on the same endpoint.

Identifying call agents by Domain Name System (DNS) name rather than by IP address in the **mgcp call-agent** and **mgcp profile call-agent** commands provides call-agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by DNS name and a message from the gateway fails to reach the call agent, the **max1 lookup** and **max2 lookup** commands enable a search from the DNS lookup table for a backup call agent at a different IP address.

The *port* argument configures the call-agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse (the gateway port number, or the UDP port over which the gateway receives messages from the call agent) is configured by specifying a port number in the **mgcp** command.

When the service type is set to **mgcp**, the call agent processes the restart in progress (RSIP) error messages sent by the gateway if the **mgcp sgcp restart notify** command is enabled. When the service type is set to **sgcp**, the call agent ignores the RSIP messages.

Use this command on any platform and media gateway.

The **mgcp** service type supports the RSIP error messages sent by the gateway if the **mgcp sgcp restart notify** command is enabled.

Examples

The following examples illustrate several formats for specifying the call agent (use any one of these formats):

```
Router(config)# mgcp call-agent 209.165.200.225 service-type mgcp version 1.0
Router(config)# mgcp call-agent 10.0.0.1 2427 service-type mgcp version rfc3435-1.0
Router(config)# mgcp call-agent igloo.northpole.net service-type ncs
Router(config)# mgcp call-agent igloo.northpole.net 2009 service-type sgcp version 1.5
Router(config)# mgcp call-agent 209.165.200.225 5530 service-type tgcp
```

Related Commands

Command	Description
call-agent	Specifies a call-agent address and protocol for an MGCP profile.
debug mgcp events	Displays debug messages for MGCP events.
max1 lookup	Enables DNS lookup of the MGCP call agent address when the suspicion threshold is reached.
max2 lookup	Enables DNS lookup of the MGCP call agent address when the disconnect threshold is reached.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure an MGCP profile associated with one or more endpoints, or to configure the default profile.
mgcp sgcp restart notify	Starts RSIP message processing in the MGCP application.mgcp
sgcp restart notify	Enables the MGCP application to process SGCP-type RSIP messages.

mgcp codec

To select the codec type and its optional packetization period value, use the **mgcp codec** command in global configuration mode. To set the codec to its default value of G711 u-law, use the **no** form of this command.

mgcp codec *type* [**packetization-period** *value*]

no mgcp codec

Syntax Description

type	Type of codec supported. Valid codecs include the following: G711alaw, G711ulaw, G723ar53, G723ar63, G723r53, G723r63, G729ar8, G729br8, and G729r8.
packetization-period *value*	(Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter is not provided by the media gateway controller. The range depends on the type of codec selected: • Range for **G729** is 10 to 220 in increments of 10. • Range for **G711** is 10 to 20 in increments of 10. • Range for **G723** is 30 to 330 in increments of 10.

Command Default **G711 u-law codec**

Command Modes Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5850.

Examples The following example specifies the codec type:

```
Router(config)# mgcp codec g711alaw
```

The following example sets the codec type and packetization period:

```
Router(config)# mgcp codec g729r8 packetization-period 150
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp codec gsmamr-nb

To specify the Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec for an MGCP dial peer, use the **mgcp codec gsmamr-nb** command in dial peer voice configuration mode. To disable the GSMAMR-NB codec, use the **no** form of this command.

mgcp codec gsmamr-nb [**packetization-period 20**] [**encap rfc3267**] [**frame-format** {**bandwidth-efficient** | **octet-aligned** [**crc** | **no-crc**]}] [**modes** *modes-value*]

no mgcp codec gsmamr-nb

Syntax Description

packetization-period 20	(Optional) Sets the packetization period at 20 ms.
encap rfc3267	(Optional) Sets the encapsulation value to comply with RFC 3267.
frame-format	(Optional) Specifies a frame format. Supported values are **octet-aligned** and **bandwidth-efficient**. The default is **octet-aligned**.
crc | **no-crc**	(Optional) CRC is applicable only for **octet-aligned** frame format. If you enter **bandwidth-efficient** frame format, the **crc** | **no-crc** options are not available because they are inapplicable.
modes	(Optional) The eight speech-encoding modes (bit rates between 4.75 and 12.2 kbps) available in the GSMAMR-NB codec.
modes-value	(Optional) Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7).

Command Default

Packetization period is **20** ms.
Encapsulation is **rfc3267**.
Frame format is **octet-aligned**.
CRC is **no-crc**.
Modes value is **0-7**.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **mgcp codec gsmamr-nb** command to configure the GSMAMR-NB codec and its parameters on the Cisco AS5350XM and Cisco AS5400XM platforms.

Examples

The following example shows how to set the codec to **gsmamr-nb** and set the parameters:

```
Router(config-dial-peer)# mgcp codec gsmamr-nb packetization-period 20 encap rfc3267
frame-format octet-aligned crc
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp codec ilbc

To specify the internet Low Bandwidth Codec (iLBC) for an MGCP dial peer, use the **mgcp codec ilbc** command in dial peer voice configuration mode. To disable the iLBC, use the **no** form of this command.

mgcp codec ilbc mode *frame_size* [**packetization-period** *value*]

no mgcp codec ilbc

Syntax Description

mode *frame_size*	Specifies the iLBC operating frame mode that is encapsulated in each packet in milliseconds (ms). Valid entries are the following: • 20—20, 40, 60, 80, 100 or 120 ms frames for 15.2 kbps bit rate. Default is 20. • 30—30, 60, 90, or 120 ms frames for 13.33 kbps bit rate. Default is 30.
packetization-period *value*	(Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter are not provided by the media gateway controller. The range is 20 to120 in increments of 10.

Command Default

20ms frames for a 15.2 kbps bit rate.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The iLBC is only supported on Cisco AS5350XM and Cisco AS5400XM Universal Gateways with Voice Feature Cards (VFCs) and IP-to-IP gateways with no transcoding and conferencing.

Examples

The following example shows how to set the MGCP codec to **ilbc** and set the parameters:

```
Router(config-dial-peer)# mgcp codec ilbc mode 20 packetization-period 60
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp crypto rfc-preferred

To enable support for the media-level Session Description Protocol (SDP) a=crypto attribute on Cisco IOS Media Gateway Control Protocol (MGCP) gateways, use the **mgcp crypto rfc-preferred** command in global configuration mode. To disable support for the a=crypto attribute, use the **no** form of this command.

mgcp crypto rfc-preferred

no mgcp crypto rfc-preferred

Syntax Description

This command has no arguments or keywords.

Command Default

Support for the a=crypto attribute is not enabled on Cisco IOS MGCP gateways.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)YB2	This command was introduced.

Usage Guidelines

Cryptographic parameters for Secure RTP (SRTP) media sessions are signalled and negotiated using the crypto attribute in the SDP. Some versions of the crytpo attribute syntax set the crypto attribute name to the X-crypto keyword (a=X-crypto). RFC 4568 *Session Description Protocol (SDP) Security Descriptions for Media Streams,* defines the crypto attribute syntax, where the attribute name is set to the crypto keyword (a=crypto). You use the **mgcp crypto rfc-preferred** command to enable support for the a=crypto attribute on Cisco MGCP gateways.

When support for a=crypto is enabled, the system can choose to use the a=crypto or a=X-crypto notation, depending on the SDP received. By default, if a remote SDP is not present, all SDPs generated by the gateway use the a=crypto notation.

If the command is disabled, the gateway can understand both a=crypto or a=X-crypto in any SDP it receives. However, all SDPs generated by the gateway use the a=X-crypto notation.

You must configure the command based on the notation used by the call agent. For example, the Cisco public switched telephone network (PSTN) gateway (PGW) uses the a=crypto notation and Cisco Unified Call Manager uses the a=X-crypto notation.

Examples

The following example enables support for the SDP a=crypto attribute on the Cisco IOS MGCP gateway:

```
Router(config)# mgcp crypto rfc-preferred
```

The following is sample output from the **show mgcp** command when support for the SDP a=crypto attribute is enabled on the Cisco IOS MGCP gateway:

```
Router(config)# show mgcp

MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is NONE
MGCP Comedia check media source is DISABLED
MGCP Comedia SDP force is DISABLED
MGCP Guaranteed scheduler time is DISABLED
MGCP Disconnect delay error recovery DISABLED
MGCP support for a:crypto RFC notation is ENABLED
MGCP DNS stale threshold is 30 seconds
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, parser, and CAC.
max1 retries	Sets the MGCP suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission).
max2 retries	Set the MGCP disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission).
mgcp	Allocates resources for the MGCP and starts the MGCP daemon.
mgcp block-newcalls	Blocks new calls while maintaining existing calls.
mgcp ip-tos	Enables or disables the IP ToS for MGCP connections.
mgcp profile	Creates and configures an MGCP profile to be associated with one or more MGCP endpoints or configures the default MGCP profile.
show mgcp	Displays values for MGCP parameters.

mgcp dns stale threshold

To configure the Media Gateway Control Protocol (MGCP) Domain Name System (DNS) stale threshold, use the **mgcp dns stale threshold** command in global configuration mode. To disable the stale threshold configuration, use the **no** form of this command.

mgcp dns stale threshold *seconds*

no mgcp dns stale threshold

Syntax Description

seconds	The threshold time in seconds, that MGCP DNS values are considered stale. The range is from 0 to 600. The default is 300.

Command Default

The MGCP DNS threshold value is set to 300 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following example shows how to set the threshold stale time to 44 seconds:

```
Router(config)# mgcp dns stale threshold 44
```

Related Commands

Command	Description
show mgcp	Displays MGCP parameter details.

mgcp debug-header

To enable the display of Media Gateway Control Protocol (MGCP) module-dependent information in the debug header, use the **mgcp debug-header** command in global configuration mode. To disable the MGCP module-dependent information, use the **no** form of this command.

mgcp debug-header

no mgcp debug-header

Syntax Description

This command has no arguments or keywords.

Command Default

MGCP module-dependent information in the debug header is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command determines whether MGCP module-dependent information is displayed in the standard header for debug output.

Examples

The following example enables MGCP module-dependent information in debug headers:

```
Router(config)# mgcp debug-header
```

Related Commands

Command	Description
debug mgcp all	Enables all debug traces for MGCP.
debug mgcp endpoint	Enables debug traces for a specific MGCP endpoint.
mgcp	Starts the MGCP daemon.
show debugging	Displays the types of debugging that are enabled.
show mgcp	Displays the MGCP parameter settings.
voice call debug	Specifies the format of the debug header.

mgcp default-package

To configure the default package capability type for the media gateway, use the **mgcp default-package** command in global configuration mode. This command does not have a **no** form. To change the default package, use the **mgcp default-package** command with a different, actively supported package.

Residential Gateways

mgcp default-package {**dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package**}

Business Gateways

mgcp default-package {**atm-package** | **dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package** | **trunk-package**}

Trunking Gateways

mgcp default-package {**as-package** | **atm-package** | **dt-package** | **dtmf-package** | **gm-package** | **hs-package** | **md-package** | **mo-package** | **ms-package** | **nas-package** | **rtp-package** | **script-package** | **trunk-package**}

Syntax Description

as-package	Announcement server package.
atm-package	ATM package.
dtmf-package	DTMF package.
dt-package	DTMF trunk package (for Channel Associated Signaling (CAS) endpoints).
fxr-package	FXR package for fax transmissions.
gm-package	Generic media package.
hs-package	Handset package.
line-package	Line package.
md-package	MD package for Feature Group D (FGD) Exchange Access North American (EANA) signaling.
mo-package	MF operator services package (for CAS endpoints).
ms-package	MF wink/immediate start package (for CAS endpoints).
nas-package	Network access server package.
rtp-package	RTP package.
script-package	Script package.
trunk-package	Trunk package.

Command Default

For residential gateways: line-package
For trunking gateways: trunk-package

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	The **line-package** keyword and a distinction between residential and trunking gateways were added.
12.1(5)XM	This command was implemented on the Cisco MC3810 and Cisco 3600 series. The **atm-package**, **hs-package**, **ms-package**, **dt-package**, and **mo-package** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.3(1)	The **fxr-package** keyword was added.
12.4(4)T	The **md-package** keyword was added.

Usage Guidelines

This command is helpful when the Media Gateway Controller does not provide the package capability to be used for the specific connection.

Before selecting a package as the default, use the **show mgcp** command to ensure that the package is actively supported. If the package you want does not appear in the display, use the **mgcp package-capability** command to add the package to the supported list.

Note The CAS packages (**dt-package**, **md-package**, **mo-package**, and **ms-package**) are available only as default package options. They do not appear as options in the **mgcp package-capability** command. This is because the non-CAS packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. Each trunk is defined using the **ds0-group** command.

If only one package is actively supported, it becomes the default package.

When the FXR package is the default, the call agent omits the "fxr/" prefix on two types of requests in CRCX, MDCX, DLCX, and RQNT messages: requests to detect events ("R:<pkg>/<evt>") and requests to generate events ("S:<pkg>/<evt>"). For example, to ask for T.38 detection, the call agent sends "R:t38" in an RQNT message rather than "R:fxr/t38." Note that the "fxr/fx:" parameter to the Local Connection Options is not affected by selection of FXR as the default package and always needs the "fxr/" prefix.

Examples

The following example sets the default package:

```
Router(config)# mgcp default-package as-package
! The announcement server package type will be the new default package type.
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port
mgcp	Starts the MGCP daemon.
mgcp package-capability	Includes a specific MGCP package that is supported by the gateway.
show mgcp	Displays values for MGCP parameters.

mgcp disconnect-delay

To configure the MGCP disconnect delay error recovery mechanism, use the **mgcp disconnect-delay** command in global configuration mode. To disable error recovery, use the **no** form of this command.

mgcp disconnect-delay [**timeout** *seconds*]

no mgcp disconnect-delay

Syntax Description

timeout	(Optional) User defined timeout before the error recovery procedure is initiated.
seconds	Length of timeout, in seconds before the error recovery procedure is initiated. The range is from 2 to 15. There is no default.

Command Default

Disconnect delay error recovery is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T8, 12.4(20)T2	This command was introduced.
12.4(22)T1	This command was integrated into Cisco IOS Release 12.4(22)T1.

Usage Guidelines

When the FXS telephony endpoint disconnect request exceeds the configured timeout value for completion, the call agent continues to send MGCP messages, which cause the FXS endpoint to eventually block or unregister the gateway. To avoid this situation, configure the gateway with the **mgcp disconnect-delay** command so that the MGCP application initiates the disconnect delay error recovery procedure when the disconnect request takes too long to complete.

When the **mgcp disconnect-delay timeout** command is configured without the optional **timeout** keyword the disconnect delay error recovery mechanism is set to 7 seconds.

Examples

The following example shows the disconnect delay error recovery mechanism set to the default timeout of 7 seconds:

```
Router(config)# mgcp disconnect-delay
```

The following example shows the disconnect delay error recovery mechanism set with a user-defined 15 seconds:

```
Router(config)# mgcp disconnect-delay timeout 15
```

mgcp dtmf-relay

To ensure accurate forwarding of digits on compressed codecs, use the **mgcp dtmf-relay** command in global configuration mode. To disable this process for uncompressed codecs, use the **no** form of this command.

Voice over IP (VoIP)

mgcp dtmf-relay voip codec {**all** | **low-bit-rate**} **mode** {**cisco** | **disabled** | **nse** | **out-of-band** | **nte-gw** | **nte-ca**}

no mgcp dtmf-relay voip

Voice over AAL2 (VoAAL2)

mgcp dtmf-relay voaal2 codec [**all** | **low-bit-rate**]

no mgcp dtmf-relay voaal2

Syntax Description

voip	Specifies VoIP calls.
voaal2	Specifies voice over AAL2 (VoAAL2) calls (using Annex K type 3 packets).
codec	Specifies the MGCP DTMF relay codec configuration.
all	Specifies that dual-tone multifrequency (DTMF) relay is to be used with all voice codecs.
low-bit-rate	Specifies that the DTMF relay is to be used with only low-bit-rate voice codecs, such as G.729.
mode	Sets MGCP DTMF relay mode.
cisco	Specifies that Real-time Transport Protocol (RTP) digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as nondigit voice samples, using payload type 121.
disabled	Sets MGCP DTMF relay mode to be disabled. This keyword is available only for the **all** keyword.
nse	Specifies that named signaling event (NSE) RTP digit events are encoded using the format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples, using the payload type that is configured using the **mgcp tse payload** command.
out-of-band	Specifies that Media Gateway Control Protocol (MGCP) digit events are sent using Notify (NTFY) messages to the call agent, which plays them on the remote gateway using Request Notification (RQNT) messages with **S:** (signal playout request).
nte-gw	Specifies that RTP digit events are encoded using the named telephony event (NTE) format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples. The payload type is negotiated by the gateways before use. The configured value for payload type is presented as the preferred choice at the beginning of the negotiation.
nte-ca	Behaves similar to the **nte-gw** keyword except that the call agent's local connection options **a:** line is used to enable or disable DTMF relay.

Defaults

For the Cisco 7200 series router, the command is disabled.
For all other platforms, noncompressed codecs are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was integrated into Cisco IOS Release 12.1(5)XM and implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. The **voaal2** keyword was added.
12.2(2)XB	This command was modified. The **nte-gw** and **nte-ca** keywords were added to this command.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(2)XN	This command was integrated into Cisco IOS Release 12.2(2)XN and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. This command was implemented on the following platforms: Cisco AS5300, Cisco AS5400, Cisco AS5850, and Cisco IAD2420.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 1751 and Cisco 1760.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **disabled** keyword was added.

Usage Guidelines

Use this command to access an announcement server or a voice-mail server that cannot decode RTP packets containing DTMF digits. When the **mgcp dtmf-relay** command is active, the DTMF digits are removed from the voice stream and carried so that the server can decode the digits.

Only VoIP supports the **mode** keyword for forwarding digits on codecs.

Examples

The following example shows how to remove the DTMF tone from the voice stream and send FRF.11 with a special payload for the DTMF digits:

```
Router(config)# mgcp dtmf-relay codec mode cisco
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to configurev a codec for VoAAL2:

```
Router(config)# mgcp dtmf-relay voaal2 codec all
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to set the DTMF relay codec and mode to gateway:

```
Router(config)# mgcp dtmf-relay codec mode nte-gw
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp endpoint offset

To enable incrementing of the POTS or DS0 portion of an endpoint name when using the Network-based Call Signaling (NCS) 1.0 profile of Media Gateway Control Protocol (MGCP), use the **mgcp endpoint offset** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp endpoint offset

no mgcp endpoint offset

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used with NCS 1.0 to increment the POTS or DS0 portion of an endpoint name by 1 to minimize potential interoperability problems with call agents (media gateway controllers).

NCS 1.0 mandates that the port number of an endpoint be based on 1, and port numbering on some gateway platforms is based on 0.

When this command is configured, it offsets all endpoint names on the gateway. For example, an endpoint with a port number of aaln/0 is offset to aaln/1, and a DS0 group number of 0/0:0 is offset to 0/0:1.

Examples

The following example enables incrementing the port number portion of an endpoint name:

```
Router(config)# mgcp endpoint offset
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp explicit hookstate

To enable detection of explicit hookstates, use the **mgcp explicit hookstate** command in global configuration mode. To disable hookstate detection, use the **no** form of this command.

mgcp explicit hookstate

no mgcp explicit hookstate

Syntax Description

This command has no arguments or keywords.

Command Default

Hookstate detection is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Explicit hookstate detection is enabled by default. In this state, the gateway returns a “401 endpoint already off hook” or “402 endpoint already on hook” NACK (Not Acknowledged) response to R:hu or R:hd event requests.

If you turn hookstate detection off with the **no** form of the **mgcp explicit hookstate** command, the hookstate is not checked when the gateway receives R:hu or R:hd event requests. The gateway acknowledges (ACK) these event requests.

Examples

The following example enables hookstate detection:

```
Router(config)# mgcp explicit hookstate
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp fax rate

To establish the maximum fax rate for Media Gateway Control Protocol (MGCP) T.38 sessions, use the **mgcp fax rate** command in global configuration mode. To reset MGCP endpoints to their default fax rate, use the **no** form of this command.

mgcp fax rate {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice**}

no mgcp fax rate

Syntax Description

2400	Maximum fax transmission speed of 2400 bits per second (bps).
4800	Maximum fax transmission speed of 4800 bps.
7200	Maximum fax transmission speed of 7200 bps.
9600	Maximum fax transmission speed of 9600 bps.
12000	Maximum fax transmission speed of 12,000 bps.
14400	Maximum fax transmission speed of 14,400 bps.
voice	Highest possible transmission speed allowed by the voice codec. This is the default.

Command Default

MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**).

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to specify the maximum fax transmission rate for all MGCP endpoints in the gateway.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but use a significantly large portion of the available bandwidth. A lower transmission speed value (2400 bps, for example) provides a slower transmission speed but uses a smaller portion of the available bandwidth.

Note MGCP fax rate does not support call admission and control or bandwidth allocation.

When the MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**), all MGCP endpoints limit T.38 fax calls to this speed. For example, if the voice codec is G.711, fax transmission may occur up to 14,400 bps because 14,400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is limited to the nearest fax rate of 7200 bps.

Tip If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission will be greater than the bandwidth reserved for Resource Reservation Protocol (RSVP). The **mgcp fax rate** command sets a maximum fax rate for T.30 negotiation (DIS/DCS). Fax machines can negotiate a lower rate, but not a higher rate.

Only values other than the default value appear in the saved gateway configuration.

Examples

The following example configures a maximum fax rate transmission speed of 9600 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 9600
```

The following example configures the maximum fax rate transmission speed to 12,000 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 12000
```

Related Commands

Command	Description
show call active fax	Displays the maximum fax rate for the current T.38 fax session.
show mgcp	Displays the current configuration for the MGCP fax rate.

mgcp fax-relay

To allow for the suppression of tones from the fax machine side so that Super Group 3 (SG3) fax machines can negotiate down to G3 speeds for Media Gateway Control Protocol (MGCP) fax relay, use the **mgcp fax-relay** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp fax-relay {**ans-disable** | **sg3-to-g3**}

no mgcp fax-relay {**ans-disable** | **sg3-to-g3**}

Syntax Description

ans-disable	Suppresses ANS tones from originating SG3 fax machines so that these machines can operate at G3 speeds using fax relay.
sg3-to-g3	Allows SG3 machines to negotiate down to G3 speeds using fax relay.

Command Default

If this command is not enabled, modem upspeed can occur when ANS tones are detected and SG3-to-SG3 fax relay communication is not supported and probably will fail.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced as the **mgcp fax-relay sg3-to-g3** command.
12.4(6)T	This command was implemented on the Cisco 1700 series and Cisco 2800 series.
12.4(20)T1	The **ans-disable** keyword was added.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

When the **mgcp fax-relay ans-disable** command is entered, modem upspeed does not occur when an ANS tone is detected. When the **ans-disable** keyword is entered, the modem-related sessions will fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **mgcp fax-relay sg3-to-g3** command is entered, the DSP fax-relay firmware suppresses the V.8 CM tone and the fax machines negotiate down to G3 speeds for the fax stream.

Examples

The following global configuration output shows V.8 fax CM message suppression being enabled on the voice dial peer for MGCP signaling types:

```
Router(config)# mgcp fax-relay sg3-to-g3
```

Related Commands

Command	Description
fax-relay(voice-service)	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay and to enable the fax stream between two SG3 fax machines to negotiate down to G3 speeds on a VoIP dial peer.
mgcp fax t38	Specifies MGCP fax T.38 parameters.

mgcp fax t38

To configure MGCP fax T.38 parameters, use the **mgcp fax t38** command in global configuration mode. return a parameter to its default, use the **no** form of this command.

mgcp fax t38 {**ecm | gateway force | hs_redundancy** *factor* **| inhibit | ls_redundancy** *factor* **| nsf** *hexcode*}

no mgcp fax t38 {**ecm | gateway force | hs_redundancy | inhibit | ls_redundancy | nsf**}

Syntax Description

ecm	Enables error correction mode (ECM) for the gateway. By default, ECM is not enabled.
gateway force	Forces gateway-controlled T.38 fax relay using Cisco-proprietary named signaling events (NSEs) even if the capability to use T.38 and NSEs cannot be negotiated by the MGCP call agent at call setup time. The default is that force is not enabled.
hs_redundancy *factor*	Sends redundant T.38 fax packets. Refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the **hs_redundancy** parameter, the *factor* range is from 0 through 2. The default is 0 (no redundancy). **Note** Setting the **hs_redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.
inhibit	Disables use of T.38 for the gateway. By default, T.38 is enabled. **Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit** command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways using auto-cofiguration and running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit** command to use T.38 fax relay.
ls_redundancy *factor*	Sends redundant T.38 fax packets. The **ls_redundancy** parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls_redundancy** parameter, the *factor* range is from 0 through 2. Default is 0 (no redundancy).
nsf *hexcode*	Overrides the nonstandard facilities (NSF) code with the code provided using the *hexcode* argument. The *word* argument is a two-digit hexadecimal country code and a four-digit hexadecimal manufacturer code. By default, the NSF code is not overridden.

Command Default

ecm—disabled
gateway force—disabled
hs_redundancy—0
inhibit—disabled (T.38 is enabled. See note in above table.)
ls_redundancy—0
nsf—not overridden

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.
12.2(11)T2	This command was modified. The **gateway force** keyword pair was introduced.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.
12.4T	This command was modified. The **mgcp fax t38 inhibit** command was no longer configured by default for MGCP gateways that use the auto-configuration function.

Usage Guidelines Nonstandard facilities (NSF) are capabilities a particular fax manufacturer has built into a fax machine to distinguish products from each other.

To disable T.38 fax relay, use the **mgcp fax t38 inhibit** command.

Some MGCP call agents do not properly pass those portions of Session Description Protocol (SDP) messages that advertise T.38 and NSE capabilities. As a result, gateways that are controlled by these call agents are unable to use NSEs to signal T.38 fax relay to other gateways that use NSEs. The **mgcp fax t38 gateway force** command provides a way to ensure gateway-controlled T.38 fax relay and use of NSEs between an MGCP gateway and another gateway. The other gateway can be an H.323, Session Initiation Protocol (SIP), or MGCP gateway. Both gateways must be configured to use NSEs to signal T.38 fax relay mode switchover. On H.323 and SIP gateways, use the **fax protocol t38 nse force** command to specify the use of NSEs for T.38 fax relay. On MGCP gateways, use the **mgcp fax t38 gateway force** command.

Examples The following example configures the gateway to use NSEs for gateway-controlled T.38 fax relay signaling:

```
Router(config)# mgcp fax t38 gateway force
```

The following example shows that MGCP T.38 fax relay and ECM are enabled, NSF override is disabled, and low- and high-speed redundancy are set to the default value of 0:

```
Router(config)# mgcp fax t38 ecm
Router(config)# exit
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.18.195.147 2436 Initial protocol service is MGCP 0.1
MGCP block-newcalls DISABLED
MGCP send RSIP for SGCP is DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
```

```
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: CA, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 119
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer disabled
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g729r8, MGCP packetization period 10
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lmw 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence: 3
MGCP default package: dt-package
MGCP supported packages: gm-package dtmf-package trunk-package line-package
                         hs-package rtp-package as-package atm-package ms-package
                         dt-package mo-package res-package mt-package
                         dt-package mo-package res-package mt-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
```

The following example shows that NSF is overridden:

```
MGCP T.38 Fax NSF Override is ENABLED: AC04D3
```

Related Commands

Command	Description
fax protocol	Specifies fax protocol parameters on H.323 and SIP gateways.

mgcp ip qos dscp

To configure Differentiated Services Code Point (DSCP) for Media Gateway Control Protocol (MGCP) packets, use the **mgcp ip qos dscp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mgcp ip qos dscp {*dscp-value* | *af-number* | *cs-number* | **default** | **ef**} {**media** | **signaling**}

no mgcp ip qos dscp {*dscp-value* | *af-number* | *cs-number* | **default** | **ef**} {**media** | **signaling**}

Syntax Description

dscp-value	DSCP value. The range is from 0 to 63.
af-number	Assured forwarding bit pattern. The assure forwarding bit patterns are as follows: • **af11** • **af12** • **af13** • **af21** • **af22** • **af23** • **af31** • **af32** • **af33** • **af41** • **af42** • **af43** For more information, use the question mark (?) online help function.
cs-number	Class selector code point. The class selector code points are as follows: • **cs1** • **cs2** • **cs3** • **cs4** • **cs5** • **cs6** • **cs7** For more information, use the question mark (?) online help function.
default	Sets the DSCP to the default bit pattern. For more information, use the question mark (?) online help function.
ef	Sets the DSCP to the expedited forwarding bit pattern. For more information, use the question mark (?) online help function.
media	Applies DSCP to media payload packets.
signaling	Applies DSCP to signaling packets.

Command Default DSCP is applied to media payload packets and signaling packets.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines The **mgcp ip qos dscp** command is used to set the DSCP for the quality of service. This command provides voice and signaling traffic priorities.

Examples The following example shows how to configure DSCP for MGCP packets:

```
Router# configure terminal
Router(config)# mgcp ip qos dscp af31 signaling
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp ip-tos

To enable or disable the IP type of service (ToS) for media gateway control protocol (MGCP) connections, use the **mgcp ip-tos** command in global configuration mode. To restore the default, use the **no** form of this command.

mgcp ip-tos {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}

no mgcp ip-tos {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}

Syntax Description

high-reliability	High-reliability ToS.
high-throughput	High-throughput ToS.
low-cost	Low-cost ToS.
low-delay	Low-delay ToS.
rtp precedence *value*	Value of the Real-Time Transport Protocol (RTP) IP precedence bit. Range is from 0 to 7. The default is 3. **Note** In Cisco IOS Release 12.1(3)T, this parameter was **precedence** *value*.
signaling precedence *value*	IP precedence value for MGCP User Datagram Protocol (UDP) and Real-Time Transport Protocol Control Protocol (RTCP) signaling packets. Range is from 0 to 7. The default is 3.

Command Default

Services are disabled.
RTP precedence: 3
Signaling precedence: 3

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810. The **precedence** parameter was changed to **rtp precedence** and the **signaling precedence** parameter was added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Only one of the keywords in the group **high-reliability**, **high-throughput**, **low-cost**, and **low-delay** can be enabled at any given time. Enabling one keyword disables any other that was active. Enabling one of these keywords has no effect on the **precedence** value.

The **no** form of the **mgcp ip-tos** command disables the first four keywords and sets **the precedence value** back to 3.

When you configure a new value for **precedence**, the old value is erased.

Examples

The following example activates the **low-delay** keyword and disables the previous three keywords:

```
Router(config)# mgcp ip-tos high-rel
Router(config)# mgcp ip-tos high-throughput
Router(config)# mgcp ip-tos low-cost
Router(config)# mgcp ip-tos low-delay
Router(config)# mgcp ip-tos rtp precedence 4
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp lawful-intercept

To enable the lawful-intercept feature for the Media Gateway Control Protocol (MGCP), use the **mgcp lawful-intercept** command in global configuration mode. To disable the feature in mgcp, use the **no** form of this command.

mgcp lawful-intercept

no mgcp lawful-intercept

Syntax Description

This command has no arguments or keywords.

Defaults

Lawful Intercept feature is enabled in mgcp.

Command Modes

Global configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The Lawful Intercept feature is the process law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. By default the **lawful-intercept** feature is enabled in mgcp. The **no mgcp lawful-intercept** command is used to disable the lawful-intercept feature in mgcp.

Examples

The following example shows the electronic surveillance being disabled:

```
Router(config)# no mgcp lawful-intercept
```

Related Commands

Command	Description
debug mgcp	Enables debugging on MGCP.
show mgcp	Displays the MGCP parameter settings.

mgcp max-waiting-delay

To specify the media gateway control protocol (MGCP) maximum waiting delay (MWD), use the **mgcp max-waiting-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp max-waiting-delay *milliseconds*

no mgcp max-waiting-delay

Syntax Description

milliseconds	Time, in milliseconds, to wait after restart. Range is from 0 to 600000 (600 seconds). The default is 3000 (3 seconds).

Command Default 3000 ms

Command Modes Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines Use this command to send out an Restart in Progress (RSIP) message to the call agent with the restart method. This command helps prevent traffic bottlenecks caused by MGCP gateways all trying to connect at the same time after a restart.

Examples The following example sets the MGCP maximum waiting delay to 600 ms:

```
Router(config)# mgcp max-waiting-delay 600
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp restart-delay	Configures the graceful teardown method sent in the RSIP message.

mgcp modem passthrough codec

To select the codec that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough codec** command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthrough {**voip** | **voaal2**} **codec** {**g711alaw** | **g711ulaw**}

no mgcp modem passthrough {**voip** | **voaal2**}

Syntax Description

voip	VoIP voice protocol.
voaal2	VoAAL2 voice protocol.
g711alaw	G.711 a-law codec for changing speeds during modem and fax switchover.
g711ulaw	G.711 u-law codec for changing speeds during modem and fax switchover.

Command Default **The g711 u-law** codec for both VOIP and VOAAL2

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. Selecting a codec dynamically changes the codec type and speed to meet network conditions.

Examples The following example enables a gateway to send and receive VoAAL2 modem or fax data using the G711 a-law codec:

```
Router(config)# mgcp modem passthrough voaal2 codec g711alaw
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.

Command	Description
mgcp quarantine persistent-events disable	Enables redundancy for VoIP modem and fax transmissions.
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthrough mode

To set the method for changing speeds that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough mode** command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthrough {**voip** | **voaal2**} **mode** {**cisco** | **nse**}

no mgcp modem passthrough {**voip** | **voaal2**}

Syntax Description

voip	VoIP.
voaal2	Voice over AAL2 calls using Annex K type 3 packets.
cisco	Cisco-proprietary method for changing modem speeds, based on the protocol.
nse	Named signaling event (NSE)-based method for changing modem speeds. For VoAAL2 configurations, AAL2 Annex K (type 3) is used.

Defaults

NSE-based method

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series router.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions.

Upspeed is the method used to change the codec type and speed dynamically to meet network conditions.

If you use the **nse** keyword, you must also use the **mgcp tse payload** command.

If you use the default **nse** keyword and the **voip** or **voaal2** keyword, the **show run** command does not display the **mgcp modem passthrough mode** command in the configuration output, although the command is displayed for the **cisco** keyword. The **show mgcp** command displays settings for both the **nse** and **cisco** keywords.

Examples

The following example enables a gateway to send and receive VoIP modem or fax data using the NSE modem-speed-changing method:

```
Router(config)# mgcp modem passthrough voip mode nse
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough codec	Selects the codec to use for modem and fax transmissions on the gateway.
mgcp quarantine persistent-events disable	Enables redundancy for VoIP modem and fax transmissions.
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthrough voip redundancy

To enable redundancy on a gateway that sends and receives modem and fax data in VoIP configurations, use the **mgcp modem passthrough voip redundancy** command in global configuration mode. To disable redundancy, use the **no** form of this command.

mgcp modem passthrough voip redundancy [**sample-duration** [**10** | **20**]] [**maximum-sessions** *number*]

no mgcp modem passthrough voip redundancy [**sample-duration** [**10** | **20**]] [**maximum-sessions** *number*]

Syntax Description

sample-duration	(Optional) Specifies the time length of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active, in milliseconds (ms).
10 | **20**	(Optional) Specifies the redundancy sample duration in milliseconds (ms). The default sample duration is 10.
maximum-sessions	(Optional) Specifies the maximum number of redundant sessions that can run simultaneously on each subsystem.
number	Number of maximum modem passthrough sessions on each module. The range is from 1 to 30.

Command Default

The default redundancy sample duration is 10 milliseconds (ms).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5300 and Cisco AS5850.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *number* argument and the following keywords were added: • **sample-duration** • **10** | **20** • **maximum-sessions**

Usage Guidelines

Use the **modem passthrough voip redundancy** command for fax pass-through because the answer tone can come from either modem or fax transmissions. This command enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss. When redundancy is on, all calls on the gateway are affected.

Upspeed is the method used to dynamically change the codec type and speed to meet network conditions.

Examples

The following example shows how to enable redundancy for VoIP modem and fax transmissions on a gateway:

```
Router(config)# mgcp modem passthrough voip redundancy sample-duration 20
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough codec	Selects the codec for modem and fax transmissions.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp tse payload	Enables the TSE payload for modem and fax operation.

mgcp modem passthru

To enable the gateway to send and receive modem and fax data, use the **mgcp modem passthru** command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

mgcp modem passthru {**cisco** | **ca**}

no mgcp modem passthru

Syntax Description

cisco	When the gateway detects a modem/fax tone, it switches the codec to G.711 to allow the analog data to pass through.
ca	When the gateway detects a modem/fax tone, it alerts the call agent to switch the codec to G.711 to allow the analog data to pass through.

Command Default **ca**

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was added to MGCP.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

When the **cisco** keyword is activated and the gateway detects a modem/fax tone, the gateway switches the codec to G.711 then sends the analog data to a remote gateway. The remote gateway also switches the codec on its side of the call to G.711 to allow the analog data to pass through.

When the **ca** keyword is activated and the gateway detects a modem/fax tone, the gateway alerts the call agent to switch the codec to G.711 to allow the analog data to pass through. The call agent must send an MDCX signal to the G.711 codec for successful data pass-through.

Examples

The following example configures a gateway to send and receive modem or fax data:

```
Router(config)# mgcp modem passthru cisco
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp modem relay voip gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip gateway-xid** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip gateway-xid [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [**string-length** *value*]

no mgcp modem relay voip gateway-xid

Syntax Description

compress	(Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled in both directions. You may want to disable compression in one or more directions. This is normally done during testing and perhaps for gaming applications, but not for normal dialup when compression is enabled in both directions. • **backward**—Enables compression only in the backward direction. • **both**—Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default. • **forward**—Enables compression only in the forward direction. • **no**—Disables compression in both directions.
dictionary *value*	(Optional) V.42bis parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.
string-length *value*	(Optional) V.42bis parameter that specifies characteristics of the compression algorithm. Range is from 16 to 32. Default is 32. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.

Command Default

Command: enabled
Compress: both
Dictionary: 1024
String length: 32

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

This command enables XID negotiation for modem relay. By default it is enabled.

This command affects only VoIP calls and not Voice over ATM adaption layer 2 (VoAAL2) calls. This is because MGCP supports VoAAL2 calls for voice and fax/modem, but not for modem relay.

If this command is enabled on both VoIP gateways of a network, the gateways determine whether they need to engage in in-band negotiation of various compression parameters. The remaining keywords in this command specify the negotiation posture of this gateway in the subsequent in-band negotiation (assuming that in-band negotiation is agreed on by the two gateways).

The **compress**, **dictionary**, and **string-length** keywords are digital-signal-processor (DSP)-specific and related to xid negotiation. If this command is disabled, they are all irrelevant. The application (MGCP or H.323) just passes these configured values to the DSPs, and it is the DSP that requires them.

Examples

The following example enables in-band negotiation of compression parameters on the VoIP gateway, with compression in both directions, dictionary size of 1024, and string length of 32 for the compression algorithm:

```
mgcp modem relay voip gateway-xid compress both dictionary 1024 string-length 32
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

mgcp modem relay voip latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip latency** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip latency *value*

no mgcp modem relay voip latency

Syntax Description

value	Estimated one-way delay across the IP network, in milliseconds. Range is from 100 to 1000. Default is 200.

Command Default 200 ms

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines Use this command to adjust the retransmission timer of the Simple Packet Relay Transport (SPRT) protocol, if required, by setting the value to the estimated one-way delay (in milliseconds) across the IP network. Changing this value may affect the throughput or delay characteristics of the modem relay call. The default value of 200 does not need to be changed for most networks.

Examples The following example sets the estimated one-way delay across the IP network to 100 ms.

```
mgcp modem relay voip latency 100
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

Command	Description
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
modem relay latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.

mgcp modem relay voip mode

To enable named signaling event (NSE) based modem relay mode for VoIP calls on a Media Gateway Control Protocol (MGCP) gateway, use the **mgcp modem relay voip mode** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip mode [**nse**] **codec** [**g711alaw** | **g711ulaw**] [**redundancy**] **gw-controlled**

no mgcp modem relay voip mode

Syntax Description

nse	(Optional) Instructs the gateway to use NSE mode for upspeeding.
codec	(Optional) Specifies a codec to use for upspeeding: • **g711alaw**—G.711 a-law 64,000 bits per second (bps) for E1. • **g711ulaw**—G.711 mu-law 64,000 bps for T1. This is the default.
redundancy	(Optional) Specifies packet redundancy for modem traffic during modem pass-through. By default, redundancy is disabled.
gw-controlled	Specifies the gateway-configured method for establishing modem relay parameters.

Command Default

Modem relay in NSE mode is disabled. All modem calls go through as pass-through calls, which are less reliable and use more bandwidth than modem relay calls, provided that pass-through is enabled.
The G.711 mu-law codec is used for upspeeding.
Redundancy is disabled and no duplicate data packets are sent while the gateway is in modem/fax pass-through mode.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(2)T	Usage guidelines were added for the **nse** keyword.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

The **mgcp modem relay voip mode** command enables non secure modem relay mode for MGCP VoIP calls. By default, NSE modem relay mode is disabled. This command configures upspeeding, which is needed because modem pass-through is an intermediate step while the gateway switches from handling voice calls to handling modem relay calls.

The **mgcp modem relay voip mode nse** command is not supported on the TI C2510 digital signal processor (DSP), formerly known as the TI C5510 DSP; only the TI C549 DSP supports negotiation of NSE parameters. If Cisco CallManager is used as the call agent, the **mgcp modem relay voip mode nse** command is not supported.

Redundancy causes the gateway to generate duplicate (redundant) data packets for fax/modem pass-through calls as per RFC 2198. For these calls to be more reliable, redundant packets transmission is needed to make up for excessive loss of packets in VoIP networks. Even if one of the gateways is configured with redundancy, calls go through. Gateways can handle asymmetric (one-way) redundancy.

To enable secure voice and data calls between Secure Telephone Equipment (STE) and IP-STE endpoints using the state signaling events (SSE) protocol, use the **mgcp modem relay voip mode sse** command. Before configuring SSE parameters, you must use the **mgcp package-capability mdste** command to enable modem relay capabilities and SSE protocol support.

The **gw-controlled** keyword specifies that modem transport parameters are configured directly on the gateway instead of being negotiated by the call agent.

Examples

The following example enables MGCP modem relay and specifies the following: NSE mode for upspeeding, G.711 mu-law codec, packet redundancy, and gateway-controlled for modem traffic during modem pass-through:

```
Router(config)# mgcp modem relay voip mode nse codec g711ulaw redundancy gw-controlled
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the modem relay transport protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode sse	Enables SSE-based modem relay.
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

mgcp modem relay voip mode sse

To enable State Signaling Event (SSE) based modem relay mode and to configure SSE parameters on the MGCP gateway, use the **mgcp modem relay voip mode sse** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip mode sse [**redundancy** [{**interval** *number* | **packet** *number*}]][**retries** *value*] [**t1** *time*]

no mgcp modem relay voip mode sse

Syntax Description

redundancy	(Optional) Packet redundancy for modem traffic during modem pass-through. By default redundancy is disabled.
interval *milliseconds*	(Optional) Specifies the timer in milliseconds (ms) for redundant transmission of SSEs. Range is 5 - 50 ms. Default is 20 ms.
packet *number*	(Optional) Specifies the SSE packet retransmission count before disconnecting. Range is 1- 5 packets. Default is 3 packets.
retries *value*	(Optional) Specifies the number of SSE packet retries, repeated every t1 interval, before disconnecting. Range is 0 - 5 retries. Default is 5 retries.
t1 *milliseconds*	(Optional) Specifies the repeat interval, in milliseconds, for initial audio SSEs used for resetting the SSE protocol state machine (clearing the call) following error recovery. Range is 500 - 3000 ms. Default is 1000 ms.

Command Default

SSE mode is enabled by default, using default parameter values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced

Usage Guidelines

Use the **mgcp modem relay voip mode sse** command to configure state signaling events (SSE) parameters for secure MGCP voice and data calls between Secure Telephone Equipment (STE) and IP STE endpoints using the SSE protocol, a subset of the V.150.1 standard for modem relay. SSEs, which are Real-Time Transport Protocol (RTP) encoded event messages, are used to coordinate transitions between the different media states, secure and nonsecure. Before configuring SSE parameters, you must use the **mgcp package-capability mdste** command to enable modem relay capabilities and SSE protocol support.

Examples

The following examples configure SSE parameters for redundancy interval redindancy packet count, number of retries and the **t1** timer interval:

```
Router(config)# mgcp modem relay voip mode sse redundancy interval 20
Router(config)# mgcp modem relay voip mode sse redundancy packet 4
Router(config)# mgcp modem relay voip mode sse retries 5
Router(config)# mgcp modem relay voip mode sse t1 1000
```

Related Commands

Command	Description
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.

mgcp modem relay voip sprt retries

To set the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting, use the **mgcp modem relay voip sprt retries** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip sprt retries *value*

no mgcp modem relay voip sprt retries

Syntax Description

value	Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12.

Command Default 12 times

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Examples The following example sets 15 as the maximum number of times that the SPRT protocol tries to send a packet before disconnecting:

```
mgcp modem relay voip sprt retries 15
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.

mgcp modem relay voip sprt v14

To configure V.14 modem relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **mgcp modem relay voip sprt v14** command in global configuration mode. To disable this function, use the **no** form of this command.

mgcp modem relay voip sprt v14 [**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*]

no mgcp modem relay voip sprt v14

Syntax Description

receive playback hold-time *milliseconds*	Configures the time in milliseconds (ms) to hold incoming data in the V.14 receive queue. Range is 20 to 250 ms. Default is 50 ms.
transmit hold-time *milliseconds*	Configures the time to wait, in ms, after the first character is ready before sending the SPRT packet. Range is 10 to 30 ms. Default is 20 ms.
transmit maximum hold-count *characters*	Configures the number of V.14 characters to be received on the ISDN public switched telephone network (PSTN) interface that will trigger sending the SPRT packet. Range is 8 to 128. Default is 16.

Command Default

V.14 modem relay parameters are enabled by default, using default parameter values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The maximum size of receive buffers is set at 500 characters, a nonprovisionable limit. Use the **mgcp modem relay voip sprt v14 receive playback hold-time** *milliseconds* command to configure the minimum holding time before characters can be removed from the receive queue. Characters received on the PSTN or ISDN interface may be collected for a configurable collection period before being sent out on SPRT channel 3, potentially resulting in variable size SPRT packets. To configure V.14 transmit parameters for SPRT packets, use the **mgcp modem relay voip sprt v14 transmit hold-time** *milliseconds* and the **mgcp modem relay voip sprt v14 transmit maximum hold-count** *characters* commands.

Parameter changes do not take effect during existing calls; they affect new calls only.

SPRT transport channel 1 is not supported.

Examples

The following example sets 200 ms as the receive playback hold time, 25 ms as the transmit hold time, and 10 characters as the transmit hold count parameters:

```
Router(config)# mgcp modem relay voip sprt v14 receive playback hold-time 200
Router(config)# mgcp modem relay voip sprt v14 transmit hold-time 25
Router(config)# mgcp modem relay voip sprt v14 transmit maximum hold-count 10
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
mgcp package-capability mdste-package	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
mgcp modem relay voip mode sse	Enables MGCP gateway SSE based modem relay mode support for VoIP calls.

mgcp package-capability

To specify the MGCP package capability type for a media gateway, use the **mgcp package-capability** command in global configuration mode. To remove a specific MGCP package capability from the list of capabilities, use the **no** form of this command.

mgcp package-capability *package*

no mgcp package-capability *package*

Syntax Description

package	One of the following package capabilities (available choices vary according to platform and release version; check the CLI help for a list): • **as-package**—Announcement server package. • **atm-package**—ATM package. MGCP for VoATM using ATM adaptation layer 2 (AAL2) permanent virtual circuit (PVC) and a subset of ATM extensions specified by Cisco is supported. Switched virtual circuit (SVC)-based VoAAL2 is not supported. • **dt-package**—Dual Tone(DT) package. Events and signals for immediate-start and basic dual tone multifrequency (DTMF) and dial-pulse trunks. • **dtmf-package**—DTMF package. Events and signals for DTMF relay. • **fxr-package**—Fax Transmission (FXR) package for fax transmissions. • **gm-package**—Generic media package. Events and signals for several types of endpoints, such as trunking gateways, access gateways, or residential gateways. • **hs-package**—Handset package. An extension of the line package, to be used when the gateway can emulate a handset. • **it-package**—PacketCable Trunking Gateway Control Protocol (TGCP) ISDN User Part (ISUP) trunk package. • **lcs-package**—MGCP Line Control Signaling (LCS) package. • **line-package**—Line package. Events and signals for residential lines. This is the default for residential gateways. • **md-package**—MD package. Provides support for Feature Group D (FGD) Exchange Access North American (EANA) protocol signaling. • **mdste-package**—Modem relay Secure Telephone Equipment (STE) package. Events and signals for modem connections enabling a secure communication path between IP-STE and STE. • **mf-package**—Multifrequency (MF) tone package. Events and signals for MF relay. • **mo-package**—Multifrequency Operations (MO) package. Events and signals for Operator Service Signaling protocol for FGD.

- **ms-package**—MS package. Events and signals for MF single-stage dialing trunks, including wink-start and immediate-start PBX Direct Inward Dialing (DID) and Direct Outward Dialing (DOD), basic R1, and FGD Terminating Protocol.
- **nas-package**—Network Access Server (NAS) Package. Accepts NAS requests from the call agent.

Note For Cisco IOS Release 12.4(4)T and later releases, the **nas-package** is not enabled by default.

- **script-package**—Script package. Events and signals for script loading.
- **srtp-package**—Secure RTP (SRTP) package. Enables the MGCP gateway to process SRTP packages. The default is disabled.
- **tone-package**—Tone package. Disabled by default. Enables the MGCP gateway to play secure call tone during midcall.
- **trunk-package**—Trunk package. Events and signals for trunk lines. This is the default for trunking gateways.

Command Default The **line-package** is configured by default for residential gateways and the **trunk package** is configured by default for trunk gateways.

Command Modes Global configuration (config)

Command History

Release	Modification
12.0(7)XR2	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(3)T	This command was implemented on the following platforms: Cisco uBR924, Cisco 2600 series, and Cisco 3660. The **line-package**, **rtp-package**, and **script-package** keywords were added and a distinction was made between residential and trunking gateways.
12.1(5)XM	This command was implemented on the Cisco 3600 series and Cisco MC3810. The **atm-package**, **dt-package, hs-package**, **mo-package,** and **ms-package** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	This command was modified. The **nat-package** and **res-package** keywords were added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3(1)	This command was modified. The **fxr-package** keyword was added.
12.3(8)T	This command was modified. The **lcs-package** keyword was added.
12.3(8)XY	This command was modified. The **pre-package** keyword was added.
12.3(11)T	This command was modified. The **srtp-package** keyword was added.

Release	Modification
12.4(2)T	This command was modified. The **mdste-package** keyword was added.
12.4(4)T	This command was modified. The **md-package** keyword was added. The **nas-package** keyword was not enabled by default.
15.1(4)M	This command was modified. The **tone-package** keyword was added.

Usage Guidelines

Events specified in the MGCP messages from the call agent must belong to one of the supported packages. Otherwise, connection requests are refused by the gateway.

By default, certain packages are configured as supported on each platform type. Using the **mgcp-package capability** command, you can configure additional package capability only for packages that are supported by your call agent. You can also disable support for a package with the **no** form of this command. Enter each package you want to add as a separate command.

Note Beginning in Cisco IOS Release12.4(4)T the **nas-package** keyword is not enabled by default.

The **md-package** keyword is enabled automatically when a T1 interface is configured to use FGD EANA signaling with the **ds0-group** command.

Use the **show mgcp** command to display the packages that are supported on the gateway.

Use this command before specifying a default package with the **mgcp default-package** command. Specify at least one default package.

Packages that are available to be configured with this command vary by platform and type of gateway. Use the CLI help to ascertain the packages available on your gateway. This example shows the CLI help output for a Cisco 3660:

```
Router# mgcp package-capability ?
as-package     Select the Announcement Server Package
atm-package    Select the ATM Package
dtmf-package   Select the DTMF Package
gm-package     Select the Generic Media Package
hs-package     Select the Handset Package
line-package   Select the Line Package
mf-package     Select the MF Package
res-package    Select the RES Package
rtp-package    Select the RTP Package
trunk-package  Select the Trunk Package
tone-package  Select the Tone Package
```

Note The Channel Associated Signaling (CAS) packages configured using the **dt-package**, **md-package**, **mo-package**, and **ms-package** keywords are available only as default packages using the **mgcp default-package** command. They do not appear as keywords in the **mgcp package-capability** command because all the other packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. The per-trunk specification is made when the trunk is configured using the **ds0-group** command.

When the **lcs-package** keyword is used on the Cisco Integrated Access Device (IAD), the named telephony events (NTEs) associated with the line control signaling (LCS) package are enabled automatically. NTEs are used by a media gateway to transport telephony tones and trunk events across a packet network. See RFC 2833.

Note Using NTE in the LCS package requires a successful MGCP/Session Definition Protocol (SDP) negotiation during call setup. The call agent must use the Line Connection Option's FMTP parameter keyword, **telephone-event**, to indicate which LCS NTEs will be used. If the IAD has been configured to use the LCS package, the IAD will answer with an SDP containing the requested LCS NTE events.

Examples

The following example enables the modem relay STE package, trunk package, DTMF package, script package, and tone package on the gateway, and then names the trunk package as the default package for the gateway:

```
Router(config)# mgcp package-capability mdste-package
Router(config)# mgcp package-capability trunk-package
Router(config)# mgcp package-capability dtmf-package
Router(config)# mgcp package-capability script-package
Router(config)# mgcp package-capability tone-package
Router(config)# mgcp default-package trunk-package
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port
mgcp	Starts the MGCP daemon.
mgcp default-package	Configures the default package capability type for the media gateway.
show mgcp	Displays the supported MGCP packages.

mgcp persistent

To configure the sending of persistent events from the Media Gateway Control Protocol (MGCP) gateway to the call agent, use the **mgcp persistent** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp persistent {**hookflash** | **offhook** | **onhook**}

no mgcp persistent {**hookflash** | **offhook** | **onhook**}

Syntax Description

hookflash	Sends persistent hookflash events to the call agent.
offhook	Sends persistent off-hook events to the call agent.
onhook	Sends persistent on-hook events to the call agent.

Command Default

The **hookflash** keyword is disabled for persistence. The **offhook** keyword is enabled for persistence. The **onhook** keyword is disabled for persistence.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Persistent events are those events that, once they are detected, are defined as reportable to the call agent whether or not the call agent has explicitly requested to be notified of their occurrence; that is, even if they are not included in the list of RequestedEvents that the gateway is asked to detect and report. Such events can include fax tones, continuity tones, and on-hook transition. Each event has an associated action for the gateway to take.

Use this command for each type of persistent event that should override the default behavior.

Examples

The following example configures the gateway to send persistent on-hook events to the call agent:

```
Router(config)# mgcp persistent onhook
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp piggyback message

To enable piggyback messages, use the **mgcp piggyback message** command in global configuration mode. To disable piggyback messages, use the **no** form of this command.

mgcp piggyback message

no mgcp piggyback message

Syntax Description This command has no arguments or keywords.

Command Default Piggyback messages are enabled

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines If the network gateway cannot handle piggyback messages, us e the **no** form of this command to disable the piggyback messages and to enable Media Gateway Control Protocol (MGCP) 1.0, Network-based Call Signaling (NCS), and Trunking Gateway Control Protocol (TGCP). Piggyback messaging is not available to Simple Gateway Control Protocol (SGCP) and MGCP 0.1.

The term piggyback message refers to a situation in which a gateway or a call agent sends more than one MGCP message in the same User Datagram Protocol (UDP) packets. The recipient processes the messages individually, in the order received. However, if a message must be retransmitted, the entire datagram is resent. The recipient must be capable of sorting out the messages and keeping track of which messages have been handled or acknowledged.

Piggybacking is used during retransmission of a message to send previously unacknowledged messages to the call agent. This maintains the order of events the call agent receives and makes sure that RestartInProgress (RSIP) messages are always received first by a call agent.

Examples The following example disables piggyback messages:

```
Router(config)# no mgcp piggyback message
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp playout

To tune the jitter-buffer packet size attempted for MGCP-controlled connections, use the **mgcp playout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp playout {**adaptive** *init-milliseconds min-milliseconds max-milliseconds* | **fax** *milliseconds* | **fixed** *milliseconds* [**no-timestamps**]}

no mgcp playout {**adaptive** | **fax** | **fixed**}

Syntax Description

adaptive *init-milliseconds min-milliseconds max-milliseconds*	Sets the range, in milliseconds (ms), for the jitter-buffer packet size. Range for each value is 4 to 250. Note that *init-milliseconds* must be between *min-milliseconds* and *max-milliseconds*. Default: 60 4 200.
fax *milliseconds*	Sets the value for the fax playout buffer size. Range: 1 to 700. Default: 300. **Note** The range and default value might vary with different platforms. See the platform digital signal processor (DSP) specifications before setting this value.
fixed *milliseconds*	Sets the fixed size, in milliseconds, for the jitter-buffer packet size. Range: 4 to 1000. There is no default value.
no-timestamps	(Optional) Fixes the jitter buffer at a constant delay without time stamps.

Command Default

The MGCP jitter playout-delay buffer is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.
12.2(13)T	This command was modified. The **fax** keyword was added.
15.1(1.8)T	This command was modified. The **no-timestamps** keyword was added and the fixed range value was increased from 250 to 1000.

Examples

The following example configures a jitter buffer to an initial playout of 100 ms, minimum buffer size of 50 ms, and maximum buffer size of 150 ms:

```
Router(config)# mgcp playout adaptive 100 50 150
```

The following example configures a fax playout buffer size of 200 ms.

```
Router(config)# mgcp playout fax 200
```

The following example configures a jitter buffer to a fixed playout of 120 ms:

```
Router(config)# mgcp playout fixed 120
```

The following example configures a jitter buffer to a fixed playout of 65 ms delay without time stamps:

```
Router(config)# mgcp playout fixed 65 no-timestamps
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
playout-delay	Tunes the playout buffer on DSPs to accommodate packet jitter caused by switches in the WAN.
playout-delay mode	Selects fixed or adaptive mode for playout delay from the jitter buffer on DSPs.

mgcp profile

To create and configure a Media Gateway Control Protocol (MGCP) profile to be associated with one or more MGCP endpoints or to configure the default MGCP profile, use the **mgcp profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

mgcp profile {*profile-name* | **default**}

no mgcp profile {*profile-name* | **default**}

Syntax Description

profile-name	Identifying name for the user-defined profile to be configured. The name can be a maximum of 32 characters.
default	The default profile is to be configured.

Command Default If this command is not used, there are no MGCP profiles created.

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.4(24)T3	The maximum number of MGCP profiles that can be configured was increased from 13 (12 plus 1 default) to 29 (28 plus 1 default).

Usage Guidelines An MGCP profile is a subset of endpoints on a media gateway. More than one MGCP profile can be configured on a gateway at the same time. Prior to Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles was 13 (12 plus 1 default). Beginning in Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles is 29 (28 plus 1 default). The **voice-port** command in MGCP profile configuration mode associates endpoints with the profile.

There are two types of MGCP parameters: global and profile-related. The parameters that are configured in MGCP profile configuration mode are the profile-related parameters. However, endpoints do not need to belong to an MGCP profile. When endpoints are not associated with any MGCP profile, values for the profile-related MGCP parameters are provided by a *default profile*. Although all of the parameters for the default profile have default values, they can also be configured in the same way that an MGCP profile is configured by simply using the **default** keyword instead of a profile name. The main difference between a default profile and a user-defined profile is that there is no voice-port or call-agent association in the default profile, but they are required in user-defined profiles. When configuring the default profile, do not use the **call-agent** command or the **voice-port** command.

This command initiates MGCP profile configuration mode, in which you create an MGCP profile for an endpoint or a set of endpoints on a media gateway, and you set parameters for that profile or for the default profile.

Examples

The following example shows the definition of the MGCP profile named newyork:

```
Router(config)# mgcp profile newyork
Router(config-mgcp-profile)# call-agent 10.14.2.200 4000 service-type mgcp version 1.0
Router(config-mgcp-profile)# voice-port 0:1
Router(config-mgcp-profile)# package persistent mt-package
Router(config-mgcp-profile)# timeout tsmax 100
Router(config-mgcp-profile)# timeout tdinit 30
Router(config-mgcp-profile)# timeout tcrit 600
Router(config-mgcp-profile)# timeout tpar 600
Router(config-mgcp-profile)# timeout thist 60
Router(config-mgcp-profile)# timeout tone mwi 600
Router(config-mgcp-profile)# timeout tone ringback 600
Router(config-mgcp-profile)# timeout tone ringback connection 600
Router(config-mgcp-profile)# timeout tone network congestion 600
Router(config-mgcp-profile)# timeout tone busy 600
Router(config-mgcp-profile)# timeout tone dial 600
Router(config-mgcp-profile)# timeout tone dial stutter 600
Router(config-mgcp-profile)# timeout tone ringing 600
Router(config-mgcp-profile)# timeout tone ringing distinctive 600
Router(config-mgcp-profile)# timeout tone reorder 600
Router(config-mgcp-profile)# timeout tone cot1 600
Router(config-mgcp-profile)# timeout tone cot2 600
Router(config-mgcp-profile)# max1 retries 10
Router(config-mgcp-profile)# no max2 lookup
Router(config-mgcp-profile)# max2 retries 10
Router(config-mgcp-profile)# exit
```

Related Commands

Command	Description
call-agent	Defines the call agent for an MGCP profile.
mgcp	Starts and allocates resources for the MGCP daemon.
voice-port	Enters voice-port configuration mode.

mgcp quality-threshold

To set the jitter buffer size threshold, latency threshold, and packet-loss threshold parameters, use the **mgcp quality-threshold** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}

no mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}

Syntax Description

hwm-cell-loss *value*	High-water-mark cell loss count, when the ATM package is enabled. Range is from 5000 to 25000. Default is 10000.
hwm-jitter-buffer *value*	High-water-mark jitter buffer size, in milliseconds. Range is from 100 to 200. Default is 150.
hwm-latency *value*	High-water-mark latency value, in milliseconds. Range is from 250 to 400. Default is 300.
hwm-packet-loss *value*	High-water-mark packet loss value, in milliseconds. Range is from 5000 to 25,000. Default is 10000.
lwm-cell-loss *value*	Low-water-mark cell loss count, when the ATM package is enabled. Range is from 1 to 3000. Default is 1000.
lwm-jitter-buffer *value*	Low-water-mark jitter buffer size, in milliseconds. Range is from 4 to 60. Default is 30.
lwm-latency *value*	Low-water-mark latency value, in milliseconds. Range is from 125 to 200. Default is 150.
lwm-packet-loss *value*	Low-water-mark packet-loss value, in milliseconds. Range is from 1 to 3000. Default is 1000.

Command Default

High-water-mark cell loss count: 10000 cells
High-water-mark jitter buffer size: 150 ms
High-water-mark latency value: 300 ms
High-water-mark packet loss value: 10000 ms
Low-water-mark cell loss count: 1000 cells
Low-water-mark jitter buffer size: 30 ms
Low-water-mark latency value: 150 ms
Low-water-mark packet-loss value: 1000 ms

Command Modes

Global configuration

Command History

Release	Modification
11.3(3)T	The default was changed to 100 milliseconds.
12.1(1)T	This command was implemented on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810. The **hwm-cell-loss** and **lwm-cell-loss** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The following impact the quality of voice calls:

- **Cell loss** (the number of ATM cells lost during transmission)
- **Jitter buffer** (storage area containing active call voice packets that have been received from the network and are waiting to be decoded and played)
- **Latency** (network delay in sending and receiving packets)
- **Packet loss** (number of packets lost per 100,000 packets for a given call)

For good voice quality, the system should perform below the low water mark values. As the values go higher, voice quality degrades. The system generates a report when the values go above the high water marks levels. Set the high water marks and low water marks values sufficiently apart so that you receive reports on poor performance, but not so close together that you receive too much feedback.

Enter each parameter as a separate command.

Examples

The following example sets various keywords to new values:

```
Router(config)# mgcp quality-threshold hwm-jitter-buffer 100
Router(config)# mgcp quality-threshold hwm-latency 250
Router(config)# mgcp quality-threshold hwm-packet-loss 5000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp package-capability	Activates various packages on the gateway.
mgcp playout	Tunes the jitter buffer packet size.

mgcp quarantine mode

To configure the mode for Media Gateway Control Protocol (MGCP) quarantined events, use the **mgcp quarantine mode** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp quarantine mode [**discard** | **process**] [**loop** | **step**]

no mgcp quarantine mode

Syntax Description

discard	Enables discarding of quarantined events instead of processing. Observed events are not reported to the call agent, even if the call agent is ready to receive them.
loop	Enables loop mode for quarantined events instead of stepping. After receiving a request from the call agent, the gateway reports the observed events to the call agent in multiples without waiting for subsequent requests.
process	Enables processing of quarantined events instead of discarding. Observed events are reported to the call agent when the call agent is ready to receive them.
step	Enables step mode for quarantined events instead of looping. After receiving a request from the call agent, the gateway reports observed events individually to the call agent, one for each request.

Command Default

If no event is specified the default is **step**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Quarantine events are defined as events that have been detected by the gateway before the arrival of the MGCP NotificationRequest command but that have not yet been notified to the call agent. They are held in the quarantine buffer until receipt of the MGCP NotificationRequest command, when the gateway is expected to generate either one notification (step by step) or multiple notifications (loop) in response to this request (the default is exactly one), based on the configuration of the **mgcp quarantine mode** command.

This command supports backward compatibility with SGCP implementations running under the MGCP application. SGCP does not have a way to allow the call agent to control the quarantine mode. MGCP has this functionality.

When the gateway is in the notification state, the interdigit timer (Tcrit) is not started.

When the gateway receives an unsuccessful NotificationRequest, the current RequestEventList and SignalEventList are emptied. The ObservedEventList and quarantine buffer are also emptied.

Changes to the quarantine mode only take effect when the gateway is rebooted or the MGCP application is restarted.

Examples

The following example starts the MGCP application:

```
Router(config)# mgcp
```

The following example stops the MGCP application:

```
Router(config)# no mgcp
```

The following example turns on processing of quarantined events and sends observed events to the call agent:

```
Router(config)# mgcp quarantine mode process
```

The following example turns off processing of quarantined events:

```
Router(config)# no mgcp quarantine mode discard
```

The following example sends observed events to the call agent in loop mode:

```
Router(config)# mgcp quarantine mode process loop
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine persistent-event disable	Disables handling of persistent call events in the quarantine buffer.

mgcp quarantine persistent-event disable

To disable handling of persistent call events in the Media Gateway Control Protocol (MGCP) quarantine buffer, use the **mgcp quarantine persistent-events disable** command in global configuration mode. To reset to the default state, use the **no** form of this command.

mgcp quarantine persistent-event disable

no mgcp quarantine persistent-event disable

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent events are held in the events buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command enables the reporting of persistent events immediately to the call agent rather than holding the events in quarantine. Persistent events are events defined as reportable whether or not the call agent explicitly has requested to be notified of their occurrence. Quarantining means that the gateway observes events but does not report them to the call agent until the call agent indicates readiness to receive notifications. By default, all events, including persistent events, are quarantined when they are detected, even when the gateway is in a notification state. When the **mgcp quarantine persistent-event disable** command is configured, however, persistent events are reported to the call agent immediately by an MGCP Notify command.

Examples

The following example disables quarantine buffer handling of persistent events:

```
Router(config)# mgcp quarantine persistent-event disable
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine mode	Configures MGCP event quarantine buffer handling mode.

mgcp request retries

This command was added in Cisco IOS Release 12.1(1)T. Beginning in Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.2(4)T, this command is supported no longer. It has been replaced by the MGCP profile **max1 retries** and **max2 retries** commands.

mgcp request timeout

To specify how long a Media Gateway Control Protocol (MGCP) gateway waits for a call-agent response to a request before retransmitting the request, use the **mgcp request timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp request timeout {*timeout-value* | **max** *maxtimeout-value*}

no mgcp request timeout [**max**]

Syntax Description

timeout-value	Time, in milliseconds, to wait for a response to a request. Range is 1 to 10000. Default is 500.
max *maxtimeout-value*	Maximum timeout, in milliseconds. Default is 4000.

Command Default

timeout-value: 500 ms
maxtimeout-value: 4000 ms

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	The **max** keyword was added to this command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco uBR925.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The request timeout value sets the initial time period that an MGCP gateway waits for a response from the call agent before retransmitting the message. The interval doubles with each retransmission. The request timeout maximum value sets an upper limit on the timeout interval.

Examples

The following example sets a router to wait 40 ms for a reply to the first request before retransmitting and limits subsequent interval maximums to 10,000 ms (10 seconds):

```
Router(config)# mgcp request timeout 40
Router(config)# mgcp request timeout max 10000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp request retries	Specifies the number of times to retry sending the **mgcp** command.

mgcp restart-delay

To select the delay value sent in the Restart in Progress (RSIP) graceful teardown, use the **mgcp restart-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp restart-delay *value*

no mgcp restart-delay

Syntax Description

value	Restart delay value, in seconds. Range is 0 to 600. The default is 0.

Command Default 0 seconds

Command Modes Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines Use this command to send an RSIP message indicating when the connection in the gateway is to be torn down.

Examples The following example sets the restart delay to 30 seconds:

```
Router(config)# mgcp restart-delay 30
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp smax-waiting-delay	Specifies the MGCP maximum waiting delay after a restart.

mgcp rtp payload-type

To specify use of the correct Real-time Transport Protocol (RTP) payload type for backward compatibility in Media Gateway Control Protocol (MGCP) networks, use the **mgcp rtp payload-type** command in global configuration mode. To restore default values for payload types, use the **no** form of this command.

Fax and Modem Codecs

mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}

no mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}

Named Signaling and Telephony Events

mgcp rtp payload-type {**nse** | **nte**} *number*

no mgcp rtp payload-type {**nse** | **nte**}

Voice Codecs

mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**} **static**

no mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**}

Syntax Description

cisco-codec-fax-ack	Payload type for Cisco codec fax acknowledgment.
cisco-codec-fax-ind	Payload type for Cisco codec fax indication.
cisco-pcm-switch-over-alaw 127	Payload type for upspeed to the G.711 a-law codec.
cisco-pcm-switch-over-ulaw 126	Payload type for upspeed to the G.711 mu-law codec.
nse	Payload type for named signaling events (NSE).
nte	Payload type for named telephony events (NTE).
number	Indicates the payload-type value. The valid range for NSE and NTE payload is from 96 to127. Default for NSE is 100. Default for NTE is 99.
clear-channel	Payload type for clear channel codec.
g726r16	Payload type for the G.726 codec at a bit rate of 16 kbps.
g726r24	Payload type for the G.726 codec at a bit rate of 24 kbps.
static	Static payload type.

Defaults

Fax and modem codecs: static RTP payload type
Voice codecs: dynamic RTP payload range from 96 to 127 (default for NSE is 100; default for NTE is 99)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5400HPX, and Cisco AS5850.
12.4(6)T	The **nse** and **nte** named signalling and telephony events keywords were added.
12.4(15)T5	The **cisco-codec-fax-ack** and **cisco-codec-fax-ind** keywords were added.
12.4(18a)	The **cisco-codec-fax-ack** and **cisco-codec-fax-ind** keywords were added.
12.4(13f)	The **cisco-codec-fax-ack** and **cisco-codec-fax-ind** keywords were added.

Usage Guidelines

Cisco IOS Release 12.2(11)T introduced an RTP payload type negotiation for MGCP VoIP calls different from previous Cisco IOS images. To ensure interoperability between gateways using different Cisco IOS images, follow these guidelines:

- For fax and modem codecs—If either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type** command on the gateway with the later release.
- For voice codecs—If you are using a Clear Channel, G.726R16, or G.726R24 codec, and either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type** command on the gateway with the later release.

If both the originating and terminating gateways are using Cisco IOS Release 12.2(11)T or a later release, this command is not required.

The **cisco-codec-fax-ack** and **cisco-codec-fax-ind** keywords are used to change the default dynamic payload type for the Cisco fax relay feature to a different dynamic payload type.

Note NSE and NTE cannot be configured to use the same value. An error message will be generated by the command parser if the same value is entered.

Examples

The following example specifies use of dynamic RTP payload type for fax and modem calls for mu-law pulse code modulation (PCM) calls in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type cisco-pcm-switch-over-ulaw 126
```

The following example specifies use of a static RTP payload type for a G.726R16 codec in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type g726r16 static
```

The following examples configure the gateway to use RTP payload 104 for NSE events and payload 108 for NTE events. These payload types are used when the gateway is advertising capabilities via the Session Definition Protocol (SDP). If the gateway is recieving the SDP, the payload types configured in the remote SDP will be used instead.

```
Router# mgcp rtp payload-type nse 104
Router# mgcp rtp payload-type nte 108
```

Related Commands

Command	Description
mgcp codec	Selects the default codec type and its optional packetization period value.

mgcp rtp unreachable timeout

To enable detection of an unreachable remote VoIP endpoint, use the **mgcp rtp unreachable timeout** command in global configuration mode. To disable detection, use the **no** form of this command.

mgcp rtp unreachable timeout *timer-value*

no mgcp rtp unreachable timeout

Note This command replaces the previously hidden **mgcp rtp icmp timeout** command.

Syntax Description

timer-value	Time, in milliseconds, that the system waits for voice packets from the unreachable endpoint. Range is 500 to 10000.

Command Default Detection is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is useful for preventing calls from remaining open when the remote endpoint is no longer available.

For example, suppose an IP phone makes a call through a gateway to another IP phone. During the call, the call agent goes down and the remote IP phone hangs up. Normally, the call agent would tell the gateway to tear down the call. In this case, the gateway continues to treat the call as active and sends more voice packets to the remote IP phone. The remote IP phone returns Internet Control Message Protocol (ICMP) port unreachable messages to the gateway. If the **mgcp rtp unreachable timeout** command is enabled, the gateway tears down the call. If the command is disabled, the call is left open.

The *timer-value* argument tells the gateway how long to wait before tearing down the call. After receiving the ICMP the unreachable message, the gateway starts a timer. If the gateway does not receive any voice packets by the end of the timer-value period, the gateway tears down the call. If some voice packets arrive before the end of the timer-value period, the gateway resets the timer and leaves the call in active state.

Examples The following example sets the Real-Time Transport Protocol (RTP) unreachable timer to 1500 ms:

```
Router(config)# mgcp rtp unreachable timeout 1500
```

Related Commands

Command	Description
mgcp	Initiates the MGCP daemon.
mgcp timer	Configures RTP stream host detection.

mgcp rtrcac

To enable Media Control Gateway Protocol (MGCP) Service Assurance (SA) Agent Call Admission Control (CAC) on an MGCP gateway supporting VoIP, use the **mgcp rtrcac** command in global configuration mode. To disable SA Agent checking on the gateway, use the **no** form of this command.

mgcp rtrcac

no mgcp rtrcac

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use this command to initiate or disable MGCP SA Agent CAC on the MGCP gateway.

Examples

The following example enables MGCP SA Agent CAC:

```
Router(config)# mgcp rtrcac
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
mgcp	Starts and allocates resources for the MGCP daemon.
rtr responder	Enables the SA Agent Responder feature.

mgcp sched-time

To configure the scheduled timer value for Media Gateway Control Protocol (MGCP), use the **mgcp sched-time** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mgcp sched-time *milliseconds*

no mgcp sched-time

Syntax Description

milliseconds	Schedule timer value, in milliseconds (ms). The range is from 12 to 40.

Command Default

The scheduled timer value for MGCP is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **mgcp sched-time** command is used to configure the MGCP process a specified time to run before it yields to a process of a lower or the same priority. The schedule timer value must be from 12 to 40 ms, the minimum and maximum time, respectively, a process can run. This ensures that the MGCP process is not suspending too often.

Examples

The following example shows how to configure the scheduled timer value for MGCP:

```
Router# configure terminal
Router(config)# mgcp sched-time 15
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp sdp

To specify parameters for Session Definition Protocol (SDP) operation in Media Gateway Control Protocol (MGCP), use the **mgcp sdp** command in global configuration mode. To disable the parameters, use the **no** form of this command.

mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}

no mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}

Syntax Description

notation undotted	Enables undotted SDP notation for the codec string in SDP.
simple	Enables simple mode of SDP operation for MGCP.
xpc-codec	Enables initial generation of the X-pc-codec field, which is used during codec negotiation in SDP for Network-based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).

Command Default

notation undotted: disabled
simple: disabled
xpc-codec: disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	The **notation undotted** and **xpc-codec** keywords were added.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command allows you to configure SDP fields to meet the requirements of your call agent.

The **notation undotted** keyword is for the G.726-16 and G.729 codecs. The codec strings G.726-16 and G.729 are dotted notation. The codec notation format is selected dynamically in the following order of preference:

1. The notation used in SDP for MGCP packets from the call agent.
2. The notation used in the a: parameter of the Local connection option for MGCP packets from the call agent.
3. The notation set by the **mgcp sdp notation undotted** command.

The **simple** keyword, when enabled, causes the gateway not to generate the following SDP fields: o (origin and session identifier), s (session name), and t (session start time and stop time). Certain call agents require this modified SDP to send data through the network.

The **xpc-codec** keyword, in TGCP and NCS, defines a new field (X-pc-codec) in the SDP for codec negotiation. To be backward compatible with non-packet-cable SDPs, the initial generation of the X-pc-codec field is suppressed by default. However, if a received SDP contains this field, the X-pc-codec field is read and generated in response to continue with the codec negotiation.

Examples

The following example configures simple mode for SDP:

```
Router(config)# mgcp sdp simple
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp sgcp disconnect notify

To enable enhanced endpoint synchronization after a disconnected procedure in a Simple Gateway Control Protocol (SGCP) version 1.5 network, use the **mgcp sgcp disconnect notify** command in global configuration mode. To disable this feature, use the **no** form of this command.

mgcp sgcp disconnect notify

no mgcp sgcp disconnect notify

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command is used with SGCP version 1.5 to provide enhanced messaging capability for an endpoint that undergoes the disconnected procedure. It does not apply to gateways that run Media Control Gateway Protocol (MGCP) or other versions of SGCP.

An SGCP endpoint may lose communication with its call agent because the call agent is temporarily off line or because of faults in the network. When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), it attempts to restore contact. If contact is not established before the disconnected timer expires, the disconnected procedure is initiated.

The disconnected procedure consists of the endpoint sending a Restart In Progress (RSIP) message to the call agent, stating that the endpoint was disconnected and is now trying to reestablish connectivity. If the **mgcp sgcp disconnect notify** command has been configured on the gateway, a special disconnected RSIP message is sent. When contact is reestablished, the call agent may decide to audit the endpoint using an Audit Endpoint (AUEP) command with additional I, ES, and RM parameters, which are defined as follows:

- I—List of connection identifiers for current connections on the endpoint
- ES—Event state of the endpoint (off-hook or on-hook)
- RM—Restart method reason for the last RSIP (graceful, forced, restart, or disconnected)

Endpoint synchronization with the call agent is achieved by the exchange of the disconnected RSIP message and the endpoint audit.

Examples

The following example enables disconnected RSIP messaging between SGCP endpoints and a call agent:

```
Router(config)# mgcp sgcp disconnect notify
```

Related Commands

Command	Description
mgcp sgcp restart notify	Enables the MGCP application to process SGCP-type RSIP messages.
show mgcp	Displays information for MGCP and SGCP parameters.

mgcp sgcp restart notify

To trigger the Media Gateway Control Protocol (MGCP) application to process Simple Gateway Control Protocol (SGCP)-type restart in progress (RSIP) messages, use the **mgcp sgcp restart notify** command in global configuration mode. To cancel the trigger, use the **no** form of this command.

mgcp sgcp restart notify

no mgcp sgcp restart notify

Syntax Description

This command has no arguments or keywords.

Command Default

SGCP does not send any RSIP messages when the protocol type is configured as SGCP.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 3600 series.
12.1(5)XM	This command was modified for MGCP and implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command is used to send RSIP messages from the router to the SGCP call agent. The RSIP messages are used to indicate whether the T1 controller is up or down so that the call agent can synchronize with the router. RSIP messages are also sent when the **mgcp** command is entered, enabling the MGCP daemon.

Examples

The following example specifies that the system sends an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
Router(config)# mgcp sgcp restart notify
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp src-cac

To enable System Resource Check (SRC) Call Admission Control (CAC) on a Media Gateway Control Protocol (MGCP) gateway supporting VoIP, use the **mgcp src-cac** command in global configuration mode. To disable system resource checking on the gateway, use the **no** form of this command.

mgcp src-cac

no mgcp src-cac

Syntax Description

This command has no arguments or keywords.

Command Default

System resource checking is disabled.

Command Modes

Global configuration

Command History

Releases	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

When this command is entered, all system-resource checks of CPU utilization, memory utilization, and maximum number of calls are performed for every call setup or modification request received from the call agent.

Examples

The following example enables MGCP VoIP SRC CAC:

```
Router(config)# mgcp src-cac
```

Related Commands

Command	Description
call threshold global	Sets threshold values for SRC CAC parameters.
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp timer

To configure how a gateway detects the Real-Time Transport Protocol (RTP) stream host, use the **mgcp timer** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp timer {**receive-rtcp** *timer* | **net-cont-test** *timer* | **nse-response t38** *timer*}

no mgcp timer {**receive-rtcp** | **net-cont-test** }

Syntax Description

receive-rtcp *timer*	Multiples of the RTCP report transmission interval, in milliseconds. Range is 1 to 100. Default is 5.
net-cont-test *timer*	Continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls, in milliseconds. Range is from 100 to 3000. The default is 200. **Note** This keyword was previously called **rtp-nse**.
nse-response t38 *timer*	Timeout period, in milliseconds, for awaiting T.38 named signaling event (NSE) responses from a peer gateway. Range is from 100 to 3000. The default is 200.

Defaults

receive-rtcp *timer*: 5 ms
net-cont-test *timer*: 200 ms
nse-response t38 *timer*: 200 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco AS5300.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620).
12.1(5)XM	This command was modified to support Media Gateway Control Protocol (MGCP). The **rtp-nse** keyword was changed to the **net-cont-test** keyword without change of functionality.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XB	This command was modified. The **nse-response t38** option was added to support MGCP T.38.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.

Usage Guidelines

Use this command to specify the RTP Control Protocol (RTCP) transmission interval for VoIP calls and the continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls.

The **receive-rtcp** keyword is the timer used by a gateway to disconnect a VoIP call when IP connectivity is lost with the remote gateway. After receiving each RTP or RTCP packet from the remote gateway, the receiving gateway starts a timer. The period of the timer is determined by multiplying the value configured using the **mgcp timer receive-rtcp** command with the value configured using **ip rtcp report interval** command. If the timer expires before the next packet is received from the remote gateway, the receiving gateway disconnects the call and notifies the call agent.

The **net-cont-test** keyword uses the terminating gateway to verify the network connectivity with the originating gateway before ringing the called party. To do this, the terminating gateway sends a command packet to the originating gateway and starts a timed for the timer period. If the timer expires before any acknowledgement from the originating gateway is received, the terminating gateway does not ring the called party, but instead disconnects the call and alerts the call agent.

The **nse-response t38** option sets the timer for awaiting T.38 NSE responses. This timer is configured to tell the terminating gateway how long to wait for an NSE from a peer gateway. The NSE from the peer gateway can either acknowledge the switch and its readiness to accept packets or indicate that it cannot accept T.38 packets.

Examples

The following example sets the multiplication factor to 10 (or x*10, where x is the interval that is set with the ip rtcp report interval command):

```
Router(config)# mgcp timer receive-rtcp 10
```

The following example sets the net-cont-test timer to 1500 ms (1.5 seconds):

```
Router(config)# mgcp timer net-cont-test 1500
```

The following example enables MGCP fax relay and sets the gateway wait time to 300 ms for an NSE from a peer gateway:

```
Router(config)# mgcp timer nse-response t38 300
```

Related Commands

Command	Description
ip rtcp report interval	Configures the minimum interval for RTCP report transmissions.
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp tse payload	Sets the TSE payload for fax and modem calls.

mgcp tse payload

To enable inband telephony signaling events (TSEs) and specify the payload value to be used during fax and modem pass-through and network continuity tests, use the **mgcp tse payload** command in global configuration mode. To disable these signaling events, use the **no** form of this command.

mgcp tse payload *value*

no mgcp tse payload

Syntax Description

value	TSE payload value. Range is from 98 to 119. The default is 100.

Command Default 100

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco MC3810 and on the Cisco 3600 series (except the Cisco 3620).
12.1(5)XM	This command was modified to support Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS release 12.2(2)T and implemented on the Cisco 7200 series router.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3620 series, and Cisco 5300.

Usage Guidelines Because this command is disabled by default, you must specify a TSE payload value. Both gateways must have the same payload value.

If you configure the **mgcp modem passthrough mode** command using the **nse** keyword, you must configure this command.

Examples The following example sets NSE mode for VoIP modem pass-through and sets the TSE payload:

```
Router(config)# mgcp modem passthrough voip mode nse
Router(config)# mgcp tse payload 100
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.

mgcp vad

To enable voice activity detection (VAD) silence suppression for Media Gateway Control Protocol (MGCP), use the **mgcp vad** command in global configuration mode. To disable VAD silence suppression, use the **no** form of this command.

mgcp vad

no mgcp vad

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use this command to tell the MGCP gateway to turn VAD silence suppression on or off.

If VAD silence suppression is turned on, silence is not sent over the network, only audible speech. Sound quality is slightly degraded but the connection monopolizes much less bandwidth.

Examples

The following example turns VAD silence suppression on:

```
Router(config)# mgcp vad
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp validate call-agent source-ipaddr

To enable the Media Gateway Control Protocol (MGCP) application to validate that packets are received from a configured call agent, use the **mgcp validate call-agent source-ipaddr** command in global configuration mode. To disable the validation feature, use the **no** form of this command.

mgcp validate call-agent *source-ipaddr*

no mgcp validate call-agent *source-ipaddr*

Syntax Description This command has no arguments or keywords.

Command Default No validation occurs.

Command Modes Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines This command verifies that incoming packets are received from MGCP or Cisco CallManager configured call agents only. When the command is enabled, all MGCP messages received from call agents that are not configured in MGCP or Cisco CallManager are dropped. Use the **mgcp validate call-agent source-ipaddr** command in place of access lists to filter out packets from unconfigured call agents. Use the **mgcp bind control source-interface** *interface* command to restrict the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces. Use the **ccm-manager config server** *server address* command to configure the Cisco CallManager address to be used when verifying incoming packets.

Examples The following example shows that MGCP call-agent validation is enabled:

```
Router(config)# mgcp validate call-agent source-ipaddr
```

Related Commands

Command	Description
ccm-manager config server	Configures the Cisco CallManager address used in verifying incoming packets.
mgcp bind control source-interface	Restricts the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces.

Command	Description
mgcp call-agent	Configures the IP address for the primary or default Cisco CallManager server and designates the optional destination UDP port number for the specified Cisco CallManager server.
show mgcp srtp	Displays active MGCP SRTP calls.

mgcp validate domain-name

To enable validation of a hostname and domain (or a specific IP address) received as part of the endpoint name in MGCP messages against those configured on the gateway, use the **mgcp validate domain-name** command in global configuration mode. To disable Media Gateway Control Protocol (MGCP) endpoint validation, use the **no** form of this command.

mgcp validate domain-name

no mgcp validate domain-name

Syntax Description

This command has no arguments or keywords.

Defaults

Hostname and domain (or IP address) validation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(17)	The default state of this command was changed to disabled.
12.3(11)T8; 12.3(14)T5	The default state of this command was changed to disabled.
12.4(1c); 12.4(3b); 12.4(5)	The default state of this command was changed to disabled.
12.4(2)T2; 12.4(4)T1; 12.4(6)T	The default state of this command was changed to disabled.

Usage Guidelines

The **mgcp validate domain-name** command enables validation of a hostname and domain (or specific IP address) received as part of the endpoint name sent from the call agent (CA) or Cisco Unified Communications Manager against those configured on the gateway. If the hostname or domain (or IP address) is not valid, the system returns a 500 error with appropriate comment.

Use the **mgcp validate domain-name** command before configuring MGCP globally in a VoIP network. (See the *Cisco Unified CallManager and Cisco IOS Interoperability Guide* for global MGCP configuration information.)

Note Only MGCP messages received from the CA or Cisco Unified Communications Manager are validated.

You can display the current setting for MGCP domain name validation using the **show running-config** command. To show only MGCP information, limit the display output to the section on MGCP (see the "Examples" section).

Note When MGCP domain name validation is disabled, the output of the **show running-config** command does not include this command—it displays only when domain name validation is enabled. However, if your system is running a software image released before the default for this feature was changed, MGCP domain name validation is turned on by default and will appear in the **show running-config** command output only if validation is disabled.

Once you enable the MGCP validate domain name feature, you should verify that the appropriate endpoint name is included as part of incoming MGCP messages. Performing this verification helps to ensure that incoming messages with invalid hostnames, domain names, and IP addresses are rejected while valid incoming messages are still allowed to reach their target endpoint (host). Enabling this validation feature without verifying this information can cause all incoming messages, even those using valid names or addresses, to be rejected (see the "Examples" section).

Examples

The following examples show how to enable MGCP domain name validation, how to verify that validation is enabled in the running configuration, and how to verify and match the hostname, domain name, or IP address specified in incoming MGCP messages to the gateway configuration.

Use the following command to enable MGCP domain name validation:

```
Router(config)# mgcp validate domain-name
```

Use the following command to verify that MGCP domain name validation is enabled:

```
Router(config)# show running-config | section mgcp
```

or

```
Router(config)# show running-config | include mgcp validate

mgcp validate domain-name
Router(config)#
```

Use the following commands and processes to verify that hostname and domain name are configured so that all and only valid incoming messages are accepted by the gateway.

After enabling domain name validation, enable debug tracing for MGCP packets:

```
Router# debug mgcp packets

Media Gateway Control Protocol packets debugging for all endpoints is on
Router#
```

Generate a call to the gateway from a CA or Cisco Unified Communications Manager. That call will generate debug messages on the gateway so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco Unified Communications Manager):

```
Router#
*Mar 14 02:29:11.512: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---
```

```
*Mar 14 02:29:11.512: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the hostname in the incoming message (aaln/S2/SU0/0@*Router2821*.example.com) does not match the hostname of the gateway (*Router*), the message was rejected (replied to with a NACK). To resolve this, change the hostname of the gateway:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname Router2821
Router2821(config)# end
Router2821#
```

Generate another call to the gateway from the CA or Cisco Unified Communications Manager. That call will generate more debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco Unified Communications Manager):

```
*Mar 14 03:01:12.480: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---

*Mar 14 03:01:12.480: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

The validation is successful and an ACK (positive response) is sent back to the CA or Cisco Unified Communications Manager because the hostname now matches. This same process also applies to validation for the domain name. Use the following commands to set the domain name for the gateway and to view current configuration for domain name and hostname:

```
Router2821# config terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router2821(config)# ip domain-name example.com
Router2821(config)# end
Router2821# show running-config

Building configuration...
.
.
.
hostname Router2821
.
.
.
ip domain name example.com
.
.
.
.
Router2821#
```

Use the following commands and processes to verify that the IP address for the gateway is configured so that all and only valid incoming messages are accepted by the gateway:

```
Router2821# show ip interface brief

Interface                  IP-Address       OK?    Method    Status    Protocol
GigabitEthernet0/0         192.0.2.189    YES    NVRAM     up        up
Router2821#
```

Generate a call to the gateway from the CA or Cisco Unified Communications Manager. That call will generate debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco Unified Communications Manager). If the MGCP message is directed to a specific IP address instead of a domain or hostname, you will see debug messages similar to the following:

```
*Mar 14 03:16:52.356: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.190] MGCP 0.1
R: L/hd(N)
X:1
<---

*Mar 14 03:16:52.356: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the IP address specified in the incoming message (aaln/S2/SU0/0@*192.0.2.190*) does not match the IP address of the GigE 0/0 interface (*192.0.2.189*), the message was rejected (replied to with a NACK). To resolve this, change the IP address specified by the CA or Cisco Unified Communications Manager for this gateway and generate another call to this gateway. If the IP addresses match, you will see debug messages similar to the following:

```
*Mar 14 03:16:10.360: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.189] MGCP 0.1
R: L/hd(N)
X:1
<---

*Mar 14 03:16:10.364: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

Because the IP address now specified in the incoming MGCP message matches the IP address of the gateway, the message was accepted and replied to with an ACK (positive response).

Related Commands

Command	Description
mgcp call-agent	Configures the IP address for the primary or default Cisco Unified Communications Manager server and designates the optional destination UDP port number for the specified Cisco Unified Communications Manager server.
show ccm-manager	Displays a list of Cisco Unified Communications Manager servers and their current status and availability.

mgcp voice-quality-stats

To enable voice-quality statistics reporting for the Media Gateway Control Protocol (MGCP), use the **mgcp voice-quality-stats** command in global configuration mode. To turn off voice-quality statistics reporting, use the no form of this command.

mgcp voice-quality-stats [**priority**<*value*>] | [**all**]

no mgcp voice-quality-stats [**priority**<*value*>] | [**all**]

Syntax Description

priority<*value*>	Selects numeric parameters to indicate priority.
all	Selects all VQ parameters.

Command Default Voice-quality statistics reporting is turned off.

Command Modes Global configuration

Command History

Release	Modification
12.3(3)	This command was introduced.
12.4(4)T	The **priority** and **all** keywords were introduced.

Usage Guidelines

- The request for digital signal processor (DSP) statistics is controlled by the RTP Control Protocol (RTCP) statistics polling interval. The polling interval is configurable by entering the **ip rtcp report interval** command. Statistics are polled every 5 seconds by default.

Note The Cisco PGW 2200 must have a patch the supports DSP statistics in order to collect data in the call detail records (CDRs).

- This command does not generate any output on the console; it adds additional quality statistics parameters in the MGCP Delete Connection (DLCX) ACK message that is sent to the call agent.
- The keyword **priority** uses a value of 1 or 2 to indicate the priority of the parameters.

The corresponding set of VQ parameters are sent in the MGCP DLCX message based on the priority selected. Cisco IOS Release 12.4(4)T supports only priority levels 1 and 2.

Examples The following example enables voice-quality statistics reporting for MGCP:

```
Router> enable
Router# configure terminal
Router(config)# mgcp voice-quality-stats
Router(config)# end
```

The following example shows the VQ parameters selected for priority 1:

```
mgcp voice-quality-stats priority 1

16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/IN: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0,
DSP/CR: CR=0, MN=0, CT=0, TT=0,
DSP/DC: DC=0,
DSP/CS: CS=0, SC=0, TS=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0
```

The following example shows all the VQ parameters selected for the keyword **all**:

```
mgcp voice-quality-stats all

16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/PE: PC=0, IC=0, SC=0, RM=0, BO=0, EE=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/ER: RD=0, TD=0, RC=0, TC=0
DSP/IC: IC=0
DSP/EC: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0, JX=0,
DSP/KF: KF=0, AV=0, MI=0, BS=0, NB=0, FL=0,
DSP/CS: CR=0, AV=0, MN=0, MX=0, CS=0, SC=0, TS=0, DC=0,
DSP/RF: ML=0, MC=0, R1=0, R2=0, IF=0, ID=0, IE=0, BL=0, R0=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0,
DSP/DL: RT=0, ED=0
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, parser, and CAC.
ip rtcp report interval	Configures the RTCP statistics polling interval.

microcode reload controller

To reload the firmware and field programmable gate array (FPGA) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

microcode reload controller {**t1** | **e1**| **j1**} {*x*/*y*}

Syntax Description

t1	T1
e1	E1
j1	J1 controller.
x/*y*	Controller slot and unit numbers. The slash must be typed.

Command Default No microcode reload activity is initiated.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	The **j1** keyword was added.

Usage Guidelines Loopbacks in the running configuration are restored after this command is entered. If the controller is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by entering the **no loop** command from the controller configuration.

Examples The following example shows how to start the microcode reload activity:

```
Router# microcode reload controller j1 3/0

TDM-connections and network traffic will be briefly disrupted.
Proceed with reload microcode?[confirm]
Router#
*Mar  3 209.165.200.225: clk_src_link_up_down: Status of this CLK does not matter

*Mar  3 209.165.200.226: clk_src_link_up_down: Status of this CLK does not matter

*Mar  3 209.165.200.227: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state to)
*Mar  3 209.165.200.227: clk_src_link_up_down: Status of this CLK does not matter

*Mar  3 209.165.200.228: clk_src_link_up_down: Status of this CLK does not matter

*Mar  3 209.165.200.229: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state top
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter

*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
```

midcall-signaling

To configure the method used for signaling messages, use the **midcall-signaling** command in SIP configuration mode. To disable the midcall-signaling feature, use the **no** form of this command.

midcall-signaling passthru

no midcall-signaling

Syntax Description

passthru	Passes SIP messages from one IP leg to another IP leg.

Command Default

Midcall-signaling is disabled.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **midcall-signaling** command distinguishes between the way Cisco Unified Communications Express and Cisco Unified Border Element handle signaling messages. Most SIP-to-SIP video and SIP-to-SIP reinvite based supplementary services require the **midcall-signaling** command to be configured before configuring other supplementary services. Supplementary service features that are functional without configuring **midcall-signaling** include: session refresh, fax, and refer-based supplementary services. The **midcall-signaling** command is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the **midcall-signaling** command be configured. The **allow-connections sip-to-sip** command must be configured before the **midcall-signaling** command.

Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

Examples

The following example shows SIP messages configured to passthrough from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling passthru
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a Cisco Unified BE.

min-se (SIP)

To change the minimum session expiration (Min-SE) header value for all calls that use the Session Initiation Protocol (SIP) session timer, use the **min-se** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

min-se *time* **session-expires** *interval*

no min-se

Syntax Description

time	Length of time, in seconds. Range: 90 to 86400 (1 day). Default: 1800.
session-expires *interval*	Indicates the session expires time interval. Range is 90 to 86400. Default:1800.

Command Default 1800 seconds (30 minutes)

Command Modes SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(9)T	This command was modified. The default time was changed from 90 to 1800 seconds.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)T	This command was modified. The **session-expires** keyword was added.

Usage Guidelines A proxy, user-agent client, and user-agent server can all have a configured minimum value indicating the smallest session interval that they accept. If they all happen to have a different configured minimum value, the highest minimum value is used. This command sets the minimum timer that is conveyed in the Min-SE header in the initial INVITE request.

The recommended value for this command is 1800 seconds (30 minutes), which is the default value. The value cannot be set below 90 seconds because excessive INVITEs create problems for routers. Once set, the value affects all calls originated by the router.

If you do not configure the session expires interval and configure only the min-se value then the session expires interval takes the value that is configured for the min-se.

Examples The following example sets the expiration timer to 90 seconds:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# min-se 90 session-expires 1800
```

Related Commands

Command	Description
show sip-ua min-se	Shows the current value of the Min-SE header.

mmoip aaa global-password

To define a password to be used with CiscoSecure for Microsoft Windows NT when using store and forward fax, use the **mmoip aaa global-password** command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa global-password *password*

no mmoip aaa global-password *password*

Syntax Description

password	Password for CiscoSecure for Windows NT to be used with store and forward fax. The maximum length is 64 alphanumeric characters.

Command Default

No password is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

CiscoSecure for Windows NT might require a separate password in order to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Microsoft Windows NT server use this defined password.

This command applies to on-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example specifies a password (password) when CiscoSecure for Microsoft Windows NT is used with store and forward fax:

```
mmoip aaa global-password password
```

mmoip aaa method fax accounting

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) accounting with store-and-forward fax, use the **mmoip aaa method fax accounting** command in global configuration mode. To reset to the undefined state, use the **no** form of this command.

mmoip aaa method fax accounting *method-list-name*

no mmoip aaa method fax accounting *method-list-name*

Syntax Description

method-list-name	List of accounting methods to be used with store-and-forward fax.

Command Default No AAA accounting method list is defined

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines This command defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command in global configuration mode. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store-and-forward fax are applied globally.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store-and-forward fax functions when a modem card is used. It is not used with voice feature cards.

Examples The following example specifies a AAA accounting method list (called “list3”) to be used with store-and-forward fax:

```
aaa new-model
mmoip aaa method fax accounting list3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.
mmoip aaa receive-accounting enable	Enables on-ramp store-and-forward fax for AAA accounting services.

mmoip aaa method fax authentication

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) authentication with store and forward fax, use the **mmoip aaa method fax authentication** command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa method fax authentication *method-list-name*

no mmoip aaa method fax authentication *method-list-name*

Syntax Description

method-list-name	List of authentication methods to be used with store and forward fax.

Command Default

No AAA authentication method list is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command defines the name of the AAA authentication method list to be used with store and forward fax. The method list itself, which defines the type of authentication services provided for store and forward fax, is defined using the **aaa authentication** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), AAA authentication method lists used with store and forward fax are applied globally on the Cisco AS5300 universal access server.

After the authentication method lists have been defined, they are enabled by using the **mmoip aaa receive-authentication enable** command.

This command applies to both on-ramp and off-ramp store and forward fax functions.

Examples

The following example specifies a AAA authentication method list (called xyz) to be used with store and forward fax:

```
aaa new-model
mmoip aaa method fax authentication xyz
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa receive-authentication enable	Enables on-ramp store and forward fax AAA authentication services.

mmoip aaa receive-accounting enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-accounting enable** command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-accounting enable

no mmoip aaa receive-accounting enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines This command enables AAA services if an accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to on-ramp store-and-forward fax functions.

Examples The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa receive-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa receive-authentication enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-authentication enable** command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-authentication enable

no mmoip aaa receive-authentication enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

This command applies to on-ramp store-and-forward fax functions.

Examples The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa receive-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa receive-id primary

To specify the primary location from which the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing, use the **mmoip aaa receive-id primary** command in global configuration mode. To remove the definition of the account identification source, use the **no** form of this command.

mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

no mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification [ANI]) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer-id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer-dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

dial peer
No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for inbound or on-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa receive-id secondary** command.

AAA does not use these methods sequentially. If the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously—for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the primary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id primary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive-id secondary	Specifies the secondary location from which AAA retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined.

mmoip aaa receive-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined, use the **mmoip aaa receive-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the **no** form of this command.

mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

no mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer-id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer-dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer DNIS, or redialer ID be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for inbound or on-ramp user authentication with store-and-forward fax if the primary identifier has not been defined.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa receive-id primary** command.

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously—for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the DNIS captured by the redialer as the secondary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id secondary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive-id primary	Specifies the primary location where AAA retrieves its account identification information for on-ramp faxing.

mmoip aaa send-accounting enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-accounting enable** command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa send-accounting enable

no mmoip aaa send-accounting enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines This command enables AAA services if an AAA method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions when using a modem card. It is not used with voice feature cards.

Examples The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa send-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa send-authentication enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-authentication enable** command in global configuration mode. To disable off-ramp AAA services, use the **no** form of this command.

mmoip aaa send-authentication enable

no mmoip aaa send-authentication enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa send-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa send-id primary

To specify the primary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id primary** command in global configuration mode. To remove the definition of the account identification source, use the **no** form of this command.

mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

no mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account-id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope-from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope-to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa send-id secondary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id primary** command in the X-account ID field of the e-mail header. This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id primary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id primary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id primary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive-id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send-id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.

mmoip aaa send-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the **no** form of this command.

mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

no mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account-id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope-from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope-to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa send-id primary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially—meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id secondary** command in the X-account ID field of the e-mail header (if store-and-forward fax uses the defined secondary identifier). This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id secondary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id secondary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id secondary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive-id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send-id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.

mode (ATM/T1/E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

Cisco 1800, Cisco 2800, Cisco 3700, Cisco 3800 Series

mode atm

no mode atm

Cisco 1700 Series, Cisco 2600XM Platform,

mode {**atm** | **t1** | **e1**}

no mode {**atm** | **t1** | **e1**}

Cisco IAD2430

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco IAD2430 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis: • Cisco 2600 series—0. • Cisco 3660—0 or 1.

cas	(Cisco 2600 series WIC slots only) Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1. On the Cisco IAD2430 series IAD, CAS mode is not supported.
t1	Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default The controller mode is disabled.

Command Modes Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to the merged SGCP/MGCP software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420 IADs.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The keyword **aim** and the argument *aim-slot* were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Note If using the **no mode atm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

Examples

ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller dsl 3/0
Router(config-controller)# mode atm
```

T1 Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller dsl 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Configures a list of time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.

mode (T1/E1 controller)

To set the T1 or E1 controller into asynchronous transfer mode (ATM) and create an ATM interface, to set the T1 or E1 controller into T1 or E1 mode and create a logical T1 or E1 controller, or to set the T1 or E1 controller into channel-associated signaling (CAS) mode, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDB3) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. On the Cisco MC3810, ATM mode is supported only on controller 0 (T1 or E1 0). **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco MC3810 and the Cisco IAD2420 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis. For the Cisco 2600 series, the AIM slot number is 0; for the Cisco 3660, the AIM slot number is 0 or 1.
cas	(CAS mode on Cisco 2600 series WIC slots only) The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1.

t1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default No controller mode is configured.

Command Modes Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The **aim** keyword and the *aim-slot* argument were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	Support was extended on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(7)T	The support that was added in Cisco IOS Release 12.3(4)XD was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines This command has the following platform-specific usage guidelines:

- Cisco 2600 series, Cisco 3660 routers, or Cisco 3700 series that use an AIM for ATM processing must use the **mode atm aim** *aim-slot* command.
- Cisco 2600 series routers that use an AIM for DSP processing and specify DS0 groups must use the **mode cas** command if they are using WIC slots for voice. This command does not apply if network modules are being used.
- Cisco 3660 routers or Cisco 3700 series that use an AIM only for DSP resources should not use this command.

- On Cisco 2600 series routers that use WIC slots for voice, the **mode atm** command without the **aim** keyword specifies software ATM segmentation and reassembly. When the **aim** keyword is used with the **mode atm** command, the AIM performs ATM segmentation and reassembly.
- Cisco MC3810 routers cannot use the **aim** keyword.
- Cisco MC3810 routers with digital voice modules (DVMs) use some DS0s exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:
  - On E1 controllers, DS0 16 is used exclusively for either CAS or common channel signaling (CCS), depending on which mode is configured.
  - On T1 controllers, DS0 24 is used exclusively for CCS.
- Cisco MC3810—When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel group** and **tdm-group** commands, respectively.
- Cisco MC3810 is not supported in the AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series feature.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in ATM mode, the mode must be set to the same mode on both the CO and CPE sides. Both sides must be set to ATM mode.
  - If the **no mode atm** command is used to leave ATM mode, the router must be rebooted immediately to clear the mode.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CO and CPE sides.

Examples

The following example configures ATM mode on controller T1 0. This step is required for Voice over ATM.

```
Router(config)# controller T1 0
Router(config-controller)# mode atm
```

The following example configures ATM mode on controller T1 1/ 0 on a Cisco 2600 series router using an AIM in slot 0 for ATM segmentation and reassembly:

```
Router(config)# controller t1 1/0
Router(config-controller)# mode atm aim 0
```

The following example configures CAS mode on controller T1 1 on a Cisco 2600 series router:

```
Router(config)# controller T1 1
Router(config-controller)# mode cas
```

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller dsl 3/0
Router(config-controller)# mode atm
```

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller dsl 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Defines the time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode bles

To set Broadband Loop Emulation Services (BLES) mode to independent or slave mode, use the **mode bles** command in dial peer configuration mode. To disable BLES mode, use the **no** form of this command.

mode bles [**slave**]

no mode bles

Syntax Description

slave	(Optional) Acts in slave mode.

Command Default

The default mode for this command is independent mode. Using the **slave** keyword sets the mode to slave mode.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco IAD2420 series.

Usage Guidelines

This command activates BLES mode. BLES mode activates the dynamic call admission control (CAC) resource allocation and implicit channel activation and deactivation. Use the **mode bles** command to activate independent mode and the **mode bles slave** command to activate slave mode.

Examples

The following example configures BLES mode:

```
voice service voatm
session protocol aal2
mode bles
```

The following example configures slave mode in BLES mode:

```
voice service voatm
session protocol aal2
mode bles slave
```

Related Commands

Command	Description
mode atm	Places the controller into ATM mode and creates an ATM interface (ATM 0).
mode cas	Places the controller into CAS mode, which allows you to create channel groups, CAS groups, and clear channels (both data and CAS modes).

mode border-element

To enable the set of commands used in border-element configuration on the Cisco 2900 and Cisco 3900 series platforms, use the **mode border-element** command in voice service configuration mode. To disable the set of commands used in border-element configuration, use the **no** form of this command.

mode border-element

no mode border-element

Syntax Description This command has no arguments or keywords.

Command Default The **mode border-element** command is disabled by default, so the commands specific to border-element configuration are unavailable on the Cisco 2900 and Cisco 3900 series platforms.

Command Modes Voice service configuration (conf-voi-serv)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines Use this command to enable the commands used in border-element configuration on Cisco 2900 and Cisco 3900 series platforms with a universal feature set. These commands are part of the **media** command. For more information about these commands, see the **media** command in the *Cisco IOS Voice Command Reference.*

If the **mode border-element** command is not entered, border-element-related commands are not available for Cisco Unified Border Element voice connections on the Cisco 2900 and Cisco 3900 series platforms with a universal feature set. The **mode border-element** command is not available on any other platforms.

For the **mode border-element** or the **no mode border-element** command to take effect, you need to save the running-config file and reload the router after you enter the command. The command-line interface (CLI) displays the following reminder after the command is entered:

```
You need to save and reload the router for this configuration change to be effective.
```

If you do not reload the router, the **mode border-element** or **no mode border-element** command does not take effect, and the availability of the commands used in border-element configuration is not affected.

Note The **show running-config** command displays the **mode border-element** or **no mode border-element** command in its output, even if a reload has not been done and either command is not in effect.

Exampless

The following example shows how to configure mode border-element and media-monitoring capability for a maximum of 200 Cisco Unified Border Element calls:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element
Router(conf-voi-serv)# media monitoring 200
```

The following example shows how to configure the **media transcoder** command for high density on all VoIP calls:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element
Router(conf-voi-serv)# media transcoder high-density
```

The following example shows how to configure the mode border-element and media flow-around for all VoIP calls:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element
Router(config-voi-serv) media flow-around
```

Related Commands

Command	Description
codec (voice port)	Specifies voice compression.
codec complexity	Specifies call density and codec complexity based on the codec used.
media	Enables media packets to pass directly between the endpoints without the intervention of the IP-to-IP gateway and enables the incoming and outgoing IP-IP call gain/loss feature for audio call scoring on either the incoming dial peer or the outgoing dial peer.
show dial peer voice	Displays the codec setting for dial peers.
show running-config	Displays the contents of the currently running configuration file on the router.

mode ccs

To configure the T1/E1 controller to support common channel signaling (CCS) cross-connect or CCS frame forwarding, use the **mode ccs** command in global configuration mode. To disable support for CCS cross-connect or CCS frame forwarding on the controller, use the **no** form of this command.

mode ccs {**cross-connect** | **frame-forwarding**}

no mode ccs {**cross-connect** | **frame-forwarding**}

Syntax Description

cross-connect	Enables CCS cross-connect on the controller.
frame-forwarding	Enables CCS frame forwarding on the controller.

Command Default

No CCS mode is configured

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810.
12.1(2)XH	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

On Cisco 2600 Series routers and Cisco 2600XM Series routers with the AIM-ATM, AIM-VOICE-30 or AIM-ATM-VOICE-30 module installed, the channel group configuration must be removed before the **no mode ccs frame-forwarding** command is entered. This restriction does not apply to the Cisco 3600 Series routers or the Cisco 3700 Series routers.

Examples

To enable CCS cross-connect on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs cross-connect
```

To enable CCS frame forwarding on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs frame-forwarding
```

Related Commands

Command	Description
ccs connect	Configures a CCS connection on an interface configured to support CCS frame forwarding.

modem passthrough (dial peer)

To enable modem pass-through over VoIP for a specific dial peer, use the **modem passthrough** command in dial peer configuration mode. To disable modem pass-through for a specific dial peer, use the **no** form of this command.

modem passthrough {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}

no modem passthrough

Syntax Description

system	Defaults to the global configuration.
nse	Specifies that named signaling events (NSEs) are used to communicate codec switchover between gateways.
payload-type *number*	(Optional) NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. For details, refer to command-line interface (CLI) help. Default is 100.
codec	Codec selections for upspeeding.
g711ulaw	Codec G.711 u-law 64000 bits per second for T1.
g711alaw	Codec G.711 a-law 64000 bits per second for E1.
redundancy	(Optional) Enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.

Defaults

payload-type *number*:100

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use this command to enable fax pass-through over VoIP individually for a single dial peer. Use the same values for all options on originating and terminating gateways.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

The **system** keyword overrides the configuration for the dial peer and directs that the values from the global configuration are to be used for this dial peer. When the **system** keyword is used, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**.

The **modem passthrough (voice service)** command can be used to set pass-through options globally on all dial peers at one time. If the **modem passthrough (voice service)** command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)** command is used on a specific dial peer, the dial peer configuration takes precedence over the global configuration for that dial peer.

Examples

The following example configures fax pass-through over VoIP for a specific dial peer:

```
dial-peer voice 25 voip
 modem passthrough nse codec g711ulaw redundancy
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
modem passthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.

modem passthrough (voice-service)

To enable fax or modem pass-through over VoIP globally for all dial peers, use the **modem passthrough** command in voice-service configuration mode. To disable fax or modem pass-through, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series, Cisco AS5300

modem passthrough nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*]]

no modem passthrough

Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco AS5350XM, Cisco AS5400XM, Cisco VGD 1T3

modem passthrough {**nse** | **protocol**} [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [**10** | **20**]]]

no modem passthrough

Syntax Description

nse	Named signaling events (NSEs) are used to communicate codec switchover between gateways.
payload-type *number*	(Optional) NSE payload type. Range varies, but is from 96 to 119 on most platforms. For details, see the command-line interface (CLI) help. Default is 100.
codec	Codec selections for upspeed.
g711ulaw	Codec G.711 mu-law, 64000 bits per second for T1.
g711alaw	Codec G.711 A-law, 64000 bits per second for E1.
redundancy	(Optional) A single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.
maximum-sessions *sessions*	(Optional) Maximum number of simultaneous pass-through sessions. Ranges and defaults vary by platform. For details, see the CLI help.
sample-duration	(Optional) Time, in milliseconds, of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active. Keywords vary by platform, but are either **10** or **20**. Default is 10.
protocol	Session Initiation Protocol (SIP)/H.323 protocol is used to signal modem pass-through.

Command Default

The command is disabled, so no fax or modem pass-through occurs.

Command Modes

Voice-service configuration (conf-voi-serv)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **sample-duration** keyword was added.
12.4(24)T	This command was implemented on the following platforms: Cisco AS5350XM, Cisco AS5400XM, and Cisco VGD 1T3. The **protocol** keyword was added.

Usage Guidelines

Use this command to enable fax or modem pass-through over VoIP globally for all dial peers. Use the same values for all options on originating and terminating gateways.

In Cisco IOS Release 12.4(24)T, the **modem passthrough protocol** command is supported only on SIP signaling.

Note The **modem passthrough protocol** and **fax protocol** commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message.

The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol passthrough** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.

Note Even though the **modem passthrough protocol** and **fax protocol passthrough** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol** command to the **modem passthrough nse** command, the configured **fax protocol passthrough** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

The **modem passthrough (dial peer)** command can be used to set pass-through options on individual dial peers. If the **modem passthrough (voice-service)** command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)** command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that specific dial peer.

Examples

The following example configures modem pass-through for NSE payload type 101 using the G.711 mu-law codec:

```
voice service voip
 modem passthrough nse payload-type 101 codec g711ulaw redundancy maximum-sessions 1
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passthrough (dial peer)	Enables fax or modem pass-through over VoIP for a specific dial peer.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (dial peer)

To configure modem relay over VoIP for a specific dial peer, use the **modem relay** command in dial peer configuration mode. To disable modem relay over VoIP for a specific dial peer, use the **no** form of this command.

modem relay {**nse** [**payload-type** *number*] **codec** {**g711alaw** | **g711ulaw**} [**redundancy**] | **system**} **gw-controlled**

no modem relay {**nse** | **system**}

Syntax Description

nse	Named signaling event (NSE).
payload-type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711 mu-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
system	This default setting uses the global configuration parameters set with the **modem relay** command in voice-service configuration mode for VoIP.
gw-controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled.
Payload type: 100

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

This command applies to VoIP dial peers. Use this command to configure modem relay over VoIP for a specific dial peer.

Use the same codec type for the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.
- E1 requires the G.711 a-law codec.

The **system** keyword overrides the configuration for the dial peer, and the values from the **modem-relay** command in voice-service configuration mode for VoIP are used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay configured for a specific dial peer using the G.711 mu-law codec and enabling redundancy and gateway-controlled negotiation parameters:

```
Router(config-dial-peer)# modem relay nse codec g711ulaw redundancy gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passsthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
modem relay (voice-service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (voice-service)

To configure modem relay over VoIP for all connections, use the **modem relay** command in voice-service configuration mode. To disable modem relay over VoIP for all connections, use the **no** form of this command.

modem relay nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**[**maximum-sessions** *value*]] **gw-controlled**

no modem relay nse

Syntax Description

nse	Named signaling event (NSE).
payload-type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711m u-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
maximum-sessions *value*	(Optional) Maximum redundant, simultaneous modem-relay pass-through sessions. Range is from 1 to 10000. Default is 16. Recommended value for the Cisco AS5300 is 26.
gw-controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled.
Payload type: 100.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(4)T	The **gw-controlled** keyword was added.
12.4(6)T	This feature was implemented on the Cisco 1700 series and Cisco 2800 series.

Usage Guidelines

Use this command to configure modem relay over VoIP. The default behavior for this command is **no modem relay**. Configuration of modem relay for VoIP dial peers via the **modem relay** dial peer configuration command overrides this voice-service command for the specific VoIP dial peer on which the dial-peer command is configured.

Use the same payload-type number for both the originating and terminating gateways.

Use the same codec type for the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.
- E1 requires the G.711 a-law codec.

The **maximum-sessions** keyword is an optional parameter for the **modem relay** command. This parameter determines the maximum number of redundant, simultaneous modem relay sessions. The recommended value for the **maximum-sessions** keyword is 16. The value can be set from 1 to 10000. The **maximum-sessions** keyword applies only if the **redundancy** keyword is used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay enabled with NSE payload type 101 using the G.711 mu-law codec, enabling redundancy and gateway-controlled negotiation parameters:

```
Router(conf-voi-serv)# modem relay nse payload-type 101 codec g711ulaw redundancy
maximum-sessions 1 gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem relay (dial peer)	Configures modem relay on a specific VoIP dial peer.

modem relay gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways, use the **modem relay gateway-xid** command in dial peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay gateway-xid [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [string-length *value*]}

no modem relay gateway-xid

Syntax Description

compress[1]	(Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled on both directions. You may want to disable compression in one or more directions. This is normally done during testing and perhaps for gaming applications, but not for normal dialup when compression is enabled in both directions. • **backward**—Enables compression only in the backward direction. • **both**—Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default. • **forward**—Enables compression only in the forward direction. • **no**—Disables compression in both directions.
dictionary *value*	(Optional) V.42 bis parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.
string-length *value*	(Optional) V.42 bis parameter that specifies characteristics of the compression algorithm. Range is from 16 to 32. Default is 32. **Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup.

1. The **compress**, **dictionary**, and **string-length** arguments can be entered in any order.

Command Default

Command: enabled
Compress: both
Dictionary: 1024
String length: 32

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

This command enables XID negotiation for modem relay. By default it is enabled.

If this command is enabled on both VoIP gateways of a network, the gateways determine whether they need to engage in in-band negotiation of various compression parameters. The remaining keywords in this command specify the negotiation posture of this gateway in the subsequent in-band negotiation (assuming that in-band negotiation is agreed on by the two gateways).

The remaining parameters specify the negotiation posture of this gateway in the subsequent inband negotiation step (assuming inband negotiation was agreed on by the two gateways).

The **compress**, **dictionary**, and **string-length** keywords are digital-signal-processor (DSP)-specific and related to xid negotiation. If this command is disabled, they are all irrelevant. The application (MGCP or H.323) just passes these configured values to the DSPs, and it is the DSP that requires them.

Examples

The following example enables in-band negotiation of compression parameters on the VoIP gateway, with compression in both directions, dictionary size of 1024, and string length of 32 for the compression algorithm:

```
modem relay gateway-xid compress both dictionary 1024 string-length 32
```

Related Commands

Command	Description
mgcp modem relay voip gateway-xid	Optimizes the modem relay transport protocol and the estimated one-way delay across the IP network.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.

modem relay latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network, use the **modem relay latency** command in dial peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay latency *value*

no modem relay latency

Syntax Description

value	Estimated one-way delay across the IP network, in milliseconds. Range is from 100 to 1000. Default is 200.

Command Default

200 ms

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Usage Guidelines

Use this command to adjust the retransmission timer of the Simple Packet Relay Transport (SPRT) protocol, if required, by setting the value to the estimated one-way delay (in milliseconds) across the IP network. Changing this value may affect the throughput or delay characteristics of the modem relay call. The default value of 200 does not need to be changed for most networks.

Examples

The following example sets the estimated one-way delay across the IP network to 100 ms.

```
Router(config-dial-peer)# modem relay latency 100
```

Related Commands

Command	Description
mgcp modem relay voip latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using MGCP.
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp modem relay voip sprt retries	Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.

Command	Description
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.

modem relay sprt retries

To set the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting, use the **modem relay sprt retries** command in dial peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt retries *value*

no modem relay sprt retries

Syntax Description

value	Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12.

Command Default

12 times

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.

Examples

The following example sets 15 as the maximum number of times that the SPRT protocol tries to send a packet before disconnecting.

```
modem relay sprt retries 15
```

Related Commands

Command	Description
mgcp modem relay voip mode	Enables modem relay mode support in a gateway for MGCP VoIP calls.
mgcp tse payload	Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP.
modem relay gateway-xid	Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP.
modem relay latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.

modem relay sprt v14

To configure V.14 modem-relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **modem relay sprt v14** command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt v14 [**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*]

no modem relay sprt v14

Syntax Description

receive playback hold-time *milliseconds*	(Optional) Configures the time in milliseconds (ms) to hold incoming data in the V.14 receive queue. Range is 20 to 250 ms. Default is 50 ms.
transmit hold-time *milliseconds*	(Optional) Configures the time to wait, in ms, after the first character is ready before sending the SPRT packet. Range is 10 to 30 ms. Default is 20 ms.
transmit maximum hold-count *characters*	(Optional) Configures the number of V.14 characters to be received on the ISDN public switched telephone network (PSTN) interface that will trigger sending the SPRT packet. Range is 8 to 128. Default is 16.

Command Default

V.14 modem-relay parameters are enabled by default, using default parameter values.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

SPRT packets are used to reliably transport modem signals between gateways. Use the **modem relay sprt v14** command under the **voice service voip** command to configure parameters for SPRT packet transport. The maximum size of the receive buffers is set at 500 characters, a nonprovisionable limit. Use the **modem relay sprt v14 receive playback hold-time** command to configure the minimum holding time before characters can be removed from the receive queue. Characters received on the PSTN or ISDN interface may be collected for a configurable collection period before being sent out on SPRT channel 3, potentially resulting in variable size SPRT packets. To configure V.14 transmit parameters for SPRT packets, use the **modem relay sprt v14 transmit hold-time** *milliseconds* and the **modem relay sprt v14 transmit maximum hold-count** *characters* commands.

Parameter changes do not take effect during existing calls; they affect new calls only.

SPRT transport channel 1 is not supported.

Use the **stcapp register capability** *voice-port* **modem-relay** command to specify modem relay as the transport method for a specific device.

Examples

The following example shows the receive playback hold time, transmit hold time, and transmit hold count parameters:

```
Router(conf-voi-serv)# modem relay sprt v14 receive playback hold-time 200
Router(conf-voi-serv)# modem relay sprt v14 transmit hold-time 25
Router(conf-voi-serv)# modem relay sprt v14 transmit maximum hold-count 10
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

modem relay sse

To enable V.150.1 modem-relay secure calls and configure state signaling events (SSE) parameters, use the **modem relay sse** command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sse [**redundancy**] [**interval** *milliseconds*] [**packet** *number*] [**retries** *value*] [**t1** *milliseconds*]

no modem relay sse

Syntax Description

redundancy	(Optional) Specifies packet redundancy for modem traffic during modem pass-through. By default redundancy is disabled.
interval *milliseconds*	(Optional) Specifies the timer in milliseconds (ms) for redundant transmission of SSEs. Range is 5 to 50 ms. Default is 20 ms.
packet *number*	(Optional) Specifies the SSE packet retransmission count before disconnecting. Range is one to five packets. Default is three packets.
retries *value*	(Optional) Specifies the number of SSE packet retries, repeated every **t1** interval, before disconnecting. Range is zero to five retries. Default is five retries.
t1 *milliseconds*	(Optional) Specifies the repeat interval, in milliseconds, for initial audio SSEs used for resetting the SSE protocol state machine (clearing the call) following error recovery. Range is 500 to 3000 ms. Default is 1000 ms.

Command Default

Modem relay mode of operation, using the SSE protocol, is enabled by default using default parameter values.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **modem relay sse** command under the **voice service voip** command to configure SSE parameters used to negotiate the transition from voice mode to V.150.1 modem-relay mode on the digital signal processor (DSP). Secure voice and data calls through the SCCP Telephony Control Application (STCAPP) gateway connect Secure Telephone Equipment (STE) and IP-STE endpoints using the SSE protocol, a subset of the V.150.1 standard for modem relay. SSEs, which are Real-Time Transport Protocol (RTP) encoded event messages that use payload 118, are used to coordinate transitions between secure and non-secure media states.

Use the **stcapp register capability** command to specify modem transport method for secure calls.

Use the **modem relay sprt v14 receive playback hold-time** command to configure V.14 receive parameters for Simple Packet Relay Transport (SPRT) protocol packets in V.150.1 modem relay mode.

Use the **modem relay sprt v14 transmit hold-time** and **modem relay sprt v14 transmit maximum hold-count** commands to configure SPRT transmit parameters in V.150.1 modem relay mode.

Use the **mgcp modem relay voip mode sse** command to enable secure V.150.1 modem relay calls on trunk-side or non-STCAPP-enabled gateways. Use the **mgcp modem relay voip mode nse** command to enable nonsecure modem-relay mode; by default, NSE modem-relay mode is disabled.

Examples

The following example shows SSE parameters configured to support secure calls between IP-STE and STE endpoints:

```
Router(config-voi-serv)# modem relay sse redundancy interval 20
Router(config-voi-serv)# modem relay sse redundancy packet 4
Router(config-voi-serv)# modem relay sse retries 5
Router(config-voi-serv)# modem relay sse t1 1000
```

Related Commands

Command	Description
mgcp package-capability mdste	Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE.
modem relay sprt v14 receive playback hold-time	Configures SPRT parameters
modem relay sprt v14 transmit hold-time	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

monitor call application event-log

To display the event log for an active application instance in real-time, use the **monitor call application event-log** command in privileged EXEC mode.

monitor call application event-log {**app-tag** *application-name* {**last** | **next**} | **session-id** *session-id* [**stop**] | **stop**}

Syntax Description

app-tag *application-name*	Displays event log for the specified application.
last	Displays event log for the most recent active instance.
next	Displays event log for the next active instance.
session-id *session-id*	Displays event log for specific application instance.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active application instances. You can view the most recent active instance or the next new instance of a specified application, or the specified active application instance, or it stops the display. To display event logs with this command, you must enable either the **call application event-log** command or the **call application voice event-log** command.

Examples

The following example displays the event log for the next active session of the application named sample_app:

```
Router# monitor call application event-log app-tag generic last

5:1057278146:172:INFO: Prompt playing finished successfully.
5:1057278151:173:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278151:174:INFO: Script received event = "noinput"
5:1057278151:175:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278158:177:INFO: Prompt playing finished successfully.
5:1057278163:178:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278163:179:INFO: Script received event = "noinput"
5:1057278163:180:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278170:182:INFO: Prompt playing finished successfully.
5:1057278175:183:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278175:184:INFO: Script received event = "noinput"
5:1057278175:185:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278181:187:INFO: Prompt playing finished successfully.

5:1057278186:188:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278186:189:INFO: Script received event = "noinput"
5:1057278186:190:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application event-log error-only	Restricts event logging to error events only for application instances.
call application voice event-log	Enables event logging for a specific voice application.
show call application session-level	Displays event logs and statistics for voice application instances.

monitor call leg event-log

To display the event log for an active call leg in real-time, use the **monitor call leg event-log** command in privileged EXEC mode.

monitor call leg event-log {**leg-id** *leg-id* [**stop**] | **next** | **stop**}

Syntax Description

leg-id *leg-id*	Displays the event log for the identified call leg.
next	Displays the event log for the next active call leg.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active voice call legs. You can view the event log for the next new call leg, or the specified active call leg, or it stops the display. To display event logs with this command, you must enable the **call leg event-log** command.

Examples

The following is sample output from the **monitor call leg event-log next** command showing the event log for the next active call leg after a PSTN incoming call was made to the gateway:

```
Router# monitor call leg event-log next

2B:1058571679:992:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
2B:1058571679:993:INFO: Dialpeer = 1
2B:1058571679:998:INFO: Digit collection
2B:1058571679:999:INFO: Call connected using codec None
2B:1058571688:1007:INFO: Call disconnected (cause = normal call clearing (16))
2B:1058571688:1008:INFO: Call released
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
show call leg	Displays event logs and statistics for voice call legs.

monitor probe icmp-ping

To enable dial-peer status changes based on the results of probes from Internet Control Message Protocol (ICMP) pings, use the **monitor probe icmp-ping** command in dial-peer configuration mode. To disable this capability, use the **no** form of this command.

monitor probe [**icmp-ping** | **rtr**] [*ip-address*]

no monitor probe [**icmp-ping** | **rtr**] [*ip-address*]

Syntax Description

icmp-ping	(Optional) Specifies ICMP ping as the method for monitoring the destination target and updating the status of the dial peer.
rtr	(Optional) Specifies that the Response Time Reporter (RTR) probe is the method for monitoring the destination target and updating the status of the dial peer.
ip-address	(Optional) The destination IP address of a target interface for the probe signal.

Command Default

If this command is not entered, no ICMP or RTR probes are sent.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.

Usage Guidelines

The principal use of this command is to specify ICMP ping as the probe method, even though the option for selecting RTR is also available.

In order for the **monitor probe icmp-ping** command to work properly, the **call fallback icmp-ping** command or the **call fallback active** command must be configured. One of these two commands must be in effect before the **monitor probe icmp-ping** command can be used.

If the **call fallback icmp-ping** command is not entered, the **call fallback active** command in global configuration is used for measurements. If the **call fallback icmp-ping** command is entered, these values override the global configuration.

Examples

The following example shows how to configure a probe to use ICMP pings to monitor the connection to IP address 10.1.1.1:

```
dial-peer voice tag voip
 call fallback icmp-ping
 monitor probe icmp-ping 10.1.1.1
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion and specifies the type of probe for pings to IP destinations.
call fallback icmp-ping	Specifies ICMP ping as the method for network traffic probe entries to IP destinations and configures parameters for the ping packets.
show voice busyout	Displays information about the voice busyout state.
voice class busyout	Creates a voice class for local voice busyout functions.

mrcp client rtpsettup enable

To enable the sending of an IP address in the Real Time Streaming Protocol (RTSP) SETUP message, use the **mrcp client rtpsettup enable** command in global configuration mode. To disable sending of the IP address, use the **no** form of this command.

mrcp client rtpsettup enable

no mrcp client rtpsettup enable

Syntax Description This command has no arguments or keywords.

Command Default This command is enabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples The following example shows how to enable the sending of IP address in the RTSP SETUP message:

```
Router# configure terminal
Router(config)# mrcp client rtpsetup enable
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client session history duration

To set the maximum number of seconds for which history records for Media Resource Control Protocol (MRCP) sessions are stored on the gateway, use the **mrcp client session history duration** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history duration *seconds*

no mrcp client session history duration

Syntax Description

seconds	Maximum time, in seconds, for which MRCP history records are stored. Range is from 0 to 99999999. The default is 3600 (1 hour). If 0 is configured, no MRCP records are stored on the gateway.

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum amount of time for which MRCP history records are stored to 2 hours (7200 seconds):

```
Router(config)# mrcp client session history duration 7200
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session history records

To set the maximum number of records of Media Resource Control Protocol (MRCP) client history that the gateway can store, use the **mrcp client session history records** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history records *number*

no mrcp client session history records

Syntax Description

number	Maximum number of MRCP history records to save. The maximum value is platform-specific. The default is 50. If 0 is configured, no MRCP records are stored on the gateway.

Command Default

50 records

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum number of MRCP records to 30:

```
Router(config)# mrcp client history records 30
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session nooffailures

To configure the maximum number of consecutive failures before disconnecting calls, use the **mrcp client session nooffailures** command in global configuration mode. To disable the number of consecutive failures before disconnecting calls, use the **no** form of this command.

mrcp client session nooffailures *number*

no mrcp client session nooffailures

Syntax Description

number	Maximum number of consecutive failures before disconnecting calls. The range is from 1 to 50. The default is 20.

Command Default

The maximum number is set to 20.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the maximum number of consecutive failures before disconnecting calls:

```
Router# configure terminal
Router(config)# mrcp client session nooffailures 20
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client statistics enable

To enable Media Resource Control Protocol (MRCP) client statistics to be displayed, use the **mrcp client statistics enable** command in global configuration mode. To disable display, use the **no** form of this command.

mrcp client statistics enable

no mrcp client statistics enable

Syntax Description

This command has no arguments or keywords.

Command Default

MRCP client statistics are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command enables MRCP client statistics to be displayed when the **show mrcp client statistics hostname** command is used. If this command is not enabled, client statistics cannot be displayed for any host when the **show mrcp client statistics hostname** command is used.

Examples

The following example enables MRCP statistics to be displayed:

```
Router(config)# mrcp client statistics enable
```

Related Commands

Command	Description
show mrcp client statistics hostname	Displays statistics about MRCP sessions for a specific MRCP host.

mrcp client timeout connect

To set the number of seconds allowed for the router to establish a TCP connection to a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout connect** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout connect *seconds*

no mrcp client timeout connect

Syntax Description

seconds	Amount of time, in seconds, the router waits to connect to the server before timing out. Range is 1 to 20.

Command Default 3 seconds

Command Modes Global configuration (global)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines This command determines when the router abandons its attempt to connect to an MRCP server and declares a timeout error, if a connection cannot be established after the specified number of seconds.

Examples The following example sets the connection timeout to 10 seconds:

```
Router(config)# mrcp client timeout connect 10
```

mrcp client timeout message

To set the number of seconds that the router waits for a response from a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout message** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout message *seconds*

no mrcp client timeout message

Syntax Description

seconds	Amount of time, in seconds, the router waits for a response from the server after making a request. Range is 1 to 20.

Command Default 3 seconds

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines This command sets the amount of time the router waits for the MRCP server to respond to a request before declaring a timeout error.

Examples The following example sets the request timeout to 10 seconds:

```
Router(config)# mrcp client timeout message 10
```

mta receive aliases

To specify a hostname accepted as a Simple Mail Transfer Protocol (SMTP) alias for off-ramp faxing, use the **mta receive aliases** command in global configuration mode. To disable the alias, use the **no** form of this command.

mta receive aliases *string*

no mta receive aliases *string*

Syntax Description

string	Hostname or IP address to be used as an alias for the SMTP server. If you specify an IP address to be used as an alias, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx]. Default is the domain name of the gateway.

Command Default Enabled with an empty string

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines This command creates an accept or reject alias list. The first alias is used by the mailer to identify itself in SMTP banners and when generating its own RFC 822 Received: header.

Note This command does not automatically include reception for a domain IP address; the address must be explicitly added. To explicitly add a domain IP address, use the following format: **mta receive aliases** [*ip-address*]. Use the IP address of the Ethernet or the FastEthernet interface of the off-ramp gateway.

This command applies to on-ramp store-and-forward fax functions.

Examples The following example specifies the host name “seattle-fax-offramp.example.com” as the alias for the SMTP server:

```
mta receive aliases seattle-fax-offramp.example.com
```

The following example specifies IP address 172.16.0.0 as the alias for the SMTP server:

```
mta receive aliases [172.16.0.0]
```

Related Commands

Command	Description
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive disable-dsn

To stop the generation and delivery of a Delivery Status Notification (DSN) every time a failure occurs in a T.37 offramp call from a Cisco IOS gateway, use the **mta receive disable-dsn** command in global configuration mode. To restart the generation and delivery of DSNs when failures occur, use the **no** form of this command.

mta receive disable-dsn

no mta receive disable-dsn

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is not enabled, and a DSN message is generated from the gateway each time a T.37 offramp call fails.

Command Modes

Global configuration

Command History

Release	Modification
12.4(13)	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The T.37 offramp gateway generates DSN messages when calls are successful and when calls fail. The **mta receive disable-dsn** command disables the generation and delivery of DSN messages for successful calls and for failed calls.

A DSN message confirming a successful call is a useful notification tool with no negative impact on processing. However, when a T.37 offramp call is made from a Cisco IOS gateway, and the call fails (ring but no answer), the gateway automatically generates a DSN for each failure. The DSN is based on the Simple Mail Transport Protocol (SMTP) error (which is temporary), so the SMTP client tries to resend the fax every 5 minutes for up to 24 hours. These multiple DSNs eventually overload the sender's inbox.

Examples

The following example shows how to disable the generation and sending of DSNs from the offramp gateway:

```
mta receive disable-dsn
```

Related Commands

Command	Description
debug fax mta	Troubleshoots the fax mail transfer agent.
mta receive generate	Specifies the type of fax delivery response message that a T.37 fax off-ramp gateway should return.

mta receive generate

Note The **mta receive generate** command replaces the **mta receive generate-mdn** command.

To specify the type of fax delivery response message that a T.37 fax off-ramp gateway should return, use the **mta receive generate** command in global configuration mode. To return to the default, use the **no** form of this command.

mta receive generate [**mdn** | **permanent-error**]

no mta receive generate [**mdn** | **permanent-error**]

Syntax Description

mdn	Optional. Directs the T.37 off-ramp gateway to process response message disposition notifications (MDNs) from an Simple Mail Transfer Protocol (SMTP) server.
permanent-error	Optional. Directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in DSN messages with descriptive error codes to an mail transfer agent (MTA).

Command Default

MDNs are not generated and standard SMTP status messages are returned to the SMTP client with error classifications of permanent or transient.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced as **mta receive generate-mdn**.
12.0(4)T	The **mta receive generate-mdn** command was integrated into Cisco IOS Release 12.0(4)T.
12.3(7)T	The **mta receive generate-mdn** command was replaced by the **mta receive generate** command, which uses the **mdn** and **permanent-error** keywords.

Usage Guidelines

When the **mdn** keyword is used to enable MDN on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate an MDN. The MDN is then returned to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device—the off-ramp gateway—to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

The **permanent-error** keyword directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in a DSN with descriptive error codes to the originating MTA. The descriptive error codes allow the MTA to control fax operations directly because the MTA can examine the error codes and make decisions about how to proceed with each fax (whether to retry or cancel, for example).

If this command is not used, the default is to return standard SMTP status messages to SMTP clients using both permanent and transient error classifications.

Examples

The following example allows a T.37 off-ramp gateway to process response MDNs:

```
Router(config)# mta receive generate mdn
```

The following example directs a T.37 off-ramp gateway to classify all fax delivery errors as permanent and forward the errors and descriptive text using SMTP DSNs to the MTA:

```
Router(config)# mta receive generate permanent-error
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when a fax-mail message is processed (opened).
mta receive aliases	Specifies a host name that is accepted as an SMTP alias for off-ramp faxing.
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive generate-mdn

Note The **mta receive generate-mdn** command was replaced by the **mta receive generate** command in Cisco IOS Release 12.3(7)T.

To specify that the off-ramp gateway process a response message disposition notification (MDN) from a Simple Mail Transfer Protocol (SMTP) server, use the **mta receive generate-mdn** command in global configuration mode. To disable MDN generation, use the **no** form of this command.

mta receive generate-mdn

no mta receive generate-mdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

When MDN is enabled on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate the MDN and return that message to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device—the off-ramp gateway—to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example enables the receiving device to generate MDNs:

```
mta receive generate-mdn
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when the fax-mail message is processed (opened).
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive maximum-recipients

To specify the maximum number of simultaneous recipients for all Simple Mail Transfer Protocol (SMTP) connections, use the **mta receive maximum-recipients** command in global configuration mode. To reset to the default, use the **no** form of this command.

mta receive maximum-recipients *number*

no mta receive maximum-recipients

Syntax Description

number	Maximum number of simultaneously recipients for all SMTP connections. Range is from 0 to 1024. The default is 0.

Command Default

0 recipients

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to configure the maximum number of resources that you want to allocate for fax usage at any one time. You can use this command to limit the resource usage on the gateway. When the value for the *number* argument is set to 0, no new connections can be established. Which is particularly useful when one is preparing to shut down the system.

This command applies to off-ramp store-and-forward fax functions.

The default of 0 recipients means that incoming mail messages are not accepted; therefore, no faxes are sent by the off-ramp gateway.

Note Unless the transmitting mailer supports the X-SESSION SMTP service extension, each incoming SMTP connection is allowed to send to only one recipient and thus consume only one outgoing voice feature card (VFC).

Examples

The following example sets the maximum number of simultaneous recipients for all SMTP connections to 10:

```
mta receive maximum-recipients 10
```

Related Commands

Command	Description
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.

mta send filename

To specify a filename for a TIFF file attached to an e-mail, use the **mta send filename** command in global configuration mode. To disable the configuration after the command has been used, use the **no** form of this command.

mta send filename [*string*] [**date**]

no mta send filename

Syntax Description

string	(Optional) Name of the TIFF file attached to an e-mail. If this text string does not contain an extension for the filename, ".tif" is added to the formatted filename.
date	(Optional) Adds today's date in the format yyyymmdd to the filename of the TIFF attachment.

Command Default The formatted filename for TIFF attachments is "Cisco_fax.tif"

Command Modes Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines Use this command to specify the filename for a TIFF file attached to an e-mail.

Examples The following example specifies a formatted filename of "abcd.tif" for the TIFF attachment:

```
Router(config)# mta send filename abcd
```

The following example specifies a formatted filename and extension of "abcd.123" for the TIFF attachment:

```
Router(config)# mta send filename abcd.123
```

The following example specifies a formatted filename "abcd_today's date" (so, for July 4, 2002, the filename would be "abcd_20020704.tif") for the TIFF attachment:

```
Router(config)# mta send filename abcd date
```

The following example specifies a formatted filename and extension of "abcd_today's date.123" (so, for July 4, 2002, the filename would be "abcd_20020704.123") for the TIFF attachment:

```
Router(config)# mta send filename abcd.123 date
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send mail-from

To specify a mail-from address (also called the RFC 821 envelope-from address or the return-path address), use the **mta send mail-from** command in global configuration mode. To remove this return-path information, use the **no** form of this command.

mta send mail-from {**hostname** *string* | **username** *string* | **username s**}

no mta send mail-from {**hostname** *string* | **username** *string* | **username s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Sender username.
username s	Wildcard that specifies that the username is derived from the calling number.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to designate the sender of the fax TIFF attachment, which is equivalent to the return path in an e-mail message. If the mail-from address is blank, the postmaster address, configured with the **mta send postmaster** command, is used.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies that the mail-from username information is derived from the calling number of the sender:

```
mta send mail-from username $s$
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send origin-prefix

To add information to an e-mail prefix header, use the **mta send origin-prefix** command in global configuration mode. To remove the defined string, use the **no** form of this command.

mta send origin-prefix *string*

no mta send origin-prefix *string*

Syntax Description

string	Text string to add comments to the e-mail prefix header. If this string contains more than one word, the string value should be enclosed within quotation marks (“abc xyz”).

Command Default Null string

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Store-and-forward fax provides the slot and port number from which an e-mail comes. In the e-mail prefix header information, use this command to define a text string to be added to the front of the e-mail prefix header information. This text string is a prefix string that is added with the modem port and slot number and passed in the originator_comment field of the esmtp_client_engine_open() call. Eventually, this text ends up in the received header field of the fax-mail message; for example:

```
Received (test onramp Santa Cruz slot1 port15) by router-5300.cisco.com for
<test-test@cisco.com> (with Cisco NetWorks); Fri, 25 Dec 1998 001500 -0800
```

Using the command **mta send origin-prefix dog** causes the received header to contain the following information:

```
Received (dog, slot 3 modem 8) by as5300-sj.example.com ....
```

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example adds information to the e-mail prefix header:

```
mta send origin-prefix "Cisco-Powered Fax System"
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send postmaster

To specify the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination, use the **mta send postmaster** command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send postmaster *e-mail-address*

no mta send postmaster *e-mail-address*

Syntax Description

e-mail-address	Address of the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to its intended destination.

Command Default

No e-mail destination is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

If you have configured a router to generate delivery status notifications (DSNs) and message disposition notifications (MDNs), but you have not configured the sender information (using the **mta send mail-from** command) or the Simple Mail Transfer Protocol (SMTP) server, DSNs and MDNs are delivered to the e-mail address determined by this command.

It is recommended that an address such as "fax-administrator@example.com" be used to indicate fax responsibility. In this example, fax-administrator is aliased to the responsible person. At some sites, this could be the same person as the e-mail postmaster, but most likely is a different person with a different e-mail address.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures the e-mail address "fax-admin@example.com" as the sender for all incoming faxes. Thus, any returned DSNs are delivered to "fax-admin@example.com" if the mail-from field is blank.

```
mta send postmaster fax-admin@example.com
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send return-receipt-to	Specifies the address to which where MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send return-receipt-to

To specify the address to which message disposition notifications (MDNs) are sent, use the **mta send return-receipt-to** command in global configuration mode. To remove the address, use the **no** form of this command.

mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}

no mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address where MDNs are sent. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Username of the sender to which MDNs are to be sent.
s	Wildcard that specifies that the calling number (ANI) generates the disposition-notification-to e-mail address.

Command Default No address is defined

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Use this command to specify where you want MDNs to be sent after a fax-mail is opened.

Note Store-and-forward fax supports the Eudora proprietary format, meaning that the header that store-and-forward fax generates is in compliance with RFC 2298 (MDN).

Note Multimedia Mail over IP (MMoIP) dial peers must have MDN enabled in order to generate return receipts in off-ramp fax-mail messages.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures “xyz” as the user and “server.com” as the SMTP mail server to which MDNs are sent:

```
mta send return-receipt-to hostname server.com
mta send return-receipt-to username xyz
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to the e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send server

To specify a destination mail server or servers, use the **mta send server** command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send server {*hostname* | *ip-address*}

no mta send server {*hostname* | *ip-address*}

Syntax Description

hostname	Hostname of the destination mail server.
ip-address	IP address of the destination mail server.

Command Default IP address defined as 0.0.0.0

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines Use this command to provide a backup destination server in case the first configured mail server is unavailable. This command is not intended to be used for load distribution.

You can configure up to ten different destination mail servers using this command. If you configure more than one destination mail server, the router attempts to contact the first mail server configured. If that mail server is unavailable, it contacts the next configured destination mail server.

DNS mail exchange (MX) records are not used to look up host names provided to this command.

Note When you use this command, configure the router to perform name lookups using the **ip name-server** command.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example defines the mail servers “xyz.example.com” and “abc.example.com” as the destination mail servers:

```
mta send server xyz.example.com
mta send server abc.example.com
```

Related Commands

Command	Description
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to the e-mail prefix header.
mta send postmaster	Specifies the mail-server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send subject	Specifies the subject header of an e-mail message.

mta send success-fax-only

To configure the router to send only successful fax messages and drop failed fax messages, use the **mta send success-fax-only** command in global configuration mode. To disable this functionality, use the **no** form of this command.

mta send success-fax-only

no mta send success-fax-only

Syntax Description

This command has no arguments or keywords.

Command Default

The router is configured to send all fax messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the router to send only successful fax messages drop failed fax messages:

```
Router# configure terminal
Router(config)# mta send success-fax-only
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.

mta send subject

To specify the subject header of an e-mail message, use the **mta send subject** command in global configuration mode. To remove the string, use the **no** form of this command.

mta send subject *string*

no mta send subject *string*

Syntax Description

string	Subject header of an e-mail message.

Command Default Null string

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines This command applies to on-ramp store-and-forward fax functions.

Note The string does not have to be enclosed in quotation marks.

Examples The following example defines the subject header of an e-mail message as “fax attachment”:

```
mta send subject fax attachment
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to an e-mail prefix header.

Command	Description
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.

mta send with-subject

To configure the subject attached with called or calling numbers, use the **mta send with-subject** command in global configuration mode. To disable the subject attached with called or calling numbers, use the **no** form of this command.

mta send with-subject {**d** | **s** | **both**}

no mta send with-subject

Syntax Description

d	Configures the subject attached with called number.
s	Configures the subject attached with calling number.
both	Configures the subject attached with both called and calling numbers.

Command Default The subject is not attached with the calling or called numbers.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines The **mta send with-subject both** command instructs the router to include the calling and called party number in the "Subject:" line of the e-mail. This helps to route the fax e-mail to the appropriate mailbox.

Examples The following example shows how to include the calling and the called party number in the "Subject:" line of the e-mail:

```
Router# configure terminal
Router(config)# mta send with-subject both
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.

music-threshold

To specify the threshold for on-hold music for a specified voice port, use the **music-threshold** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

music-threshold *decibels*

no music-threshold *decibels*

Syntax Description

decibels	On-hold music threshold, in decibels (dB). Range is from –70 to –10 (integers only). The default is –38 dB.

Command Default –38 dB

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)T	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels* argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines Use this command to specify the decibel level of music played when calls are put on hold. This command tells the firmware to pass steady data above the specified level. It affects the operation of voice activity detection (VAD) only when the voice port is receiving voice.

If the value for this command is set too high, VAD interprets music-on-hold as silence, and the remote end does not hear the music. If the value for this command is set too low, VAD compresses and passes silence when the background is noisy, creating unnecessary voice traffic.

Examples The following example sets the decibel threshold to –35 for the music played when calls are put on hold:

```
voice port 0:D
 music-threshold -35
```

The following example sets the decibel threshold to –35 for the music played when calls are put on hold on a Cisco 3600 series router:

```
voice-port 1/0/0
 music-threshold -35
```

mwi

To enable message-waiting indication (MWI) for a specified voice port, use the **mwi** command in voice-port configuration mode. To disable MWI for a specified voice port, use the **no** form of this command.

mwi

no mwi

Syntax Description This command has no arguments or keywords.

Command Default MWI is disabled by default.

Command Modes Voice-port configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines Use the **mwi** command to enable MWI functionality on the voice port and the **mwi-server** command to configure the voice-mail server to send MWI notifications. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. If there are multiple dial peers associated with the same FXS voice port, multiple subscriptions are sent to the voice-mail server.

Examples The following example shows MWI set on a voice port.

```
voice-port 2/2
 cptone us
 mwi
```

Related Commands

Command	Description
cptone	Specifies a regional analog voice-interface-related tone, ring, and cadence setting.
mwi-server	Specifies voice-mail server settings on a voice gateway or UA.
voice-port	Enters voice-port configuration mode.

mwi (supplementary-service)

To set the type of message waiting indication (MWI) when a voicemail is available, use the **mwi** command in supplementary-service configuration mode. To return to the default setting, use the **no** form of this command.

mwi {**audible** | **visible** | **both**}

no mwi

Syntax Description

audible	Audible message waiting indication (AMWI) is enabled.
visible	Visible message waiting indication (VMWI) is enabled.
both	Default configuration. Both AMWI and VMWI are enabled.

Command Default

Both AMWI and VMWI are enabled by default.

Command Modes

Supplementary-service configuration (config-stcapp-suppl-serv)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **mwi** command to enable MWI as audible only (AMVI), visible only (VMWI), or both (AMVI/VMWI).

When a voicemail is available, you go offhook to hear a special AMWI tone or you go onhook to see an MWI light (when the phone is equipped with one).

Examples

The following example shows how to set the type of MWI on voice ports 2/1, 2/2, and 2/3:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/1
Router(config-stcapp-suppl-serv-port)# fallback-dn 3001
Router(config-stcapp-suppl-serv)# port 2/2
Router(config-stcapp-suppl-serv-port)# fallback-dn 3102
Router(config-stcapp-suppl-serv-port)# mwi visible
Router(config-stcapp-suppl-serv)# port 2/3
Router(config-stcapp-suppl-serv-port)# fallback-dn 3203
Router(config-stcapp-suppl-serv-port)# mwi audible
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

mwi-server

To specify voice-mail server settings on a voice gateway or user agent (UA), use the **mwi-server** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

mwi-server {**ipv4:***destination-address* | **dns:***host-name*} [**expires** *seconds*] [**port** *port*] [**transport** {**tcp** | **udp**}] [**unsolicited**]

no mwi-server

Syntax Description

ipv4:*destination-address*	IP address of the voice-mail server.
dns:*host-name*	Host device housing the domain name server that resolves the name of the voice-mail server. • *host-name*—String that contains the complete host name to be associated with the target address; for example, **dns:test.cisco.com**.
expires *seconds*	(Optional) Subscription expiration time, in seconds. The range is 1 to 999999. The default is 3600.
port *port*	(Optional) Defines the port number on the voice-mail server. The default is 5060.
transport {**tcp** | **udp**}	(Optional) Defines the transport protocol to the voice-mail server. Choices are **tcp** or **udp**. UDP is the default.
unsolicited	(Optional) Requires the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes. Removes the requirement that the voice gateway subscribe for MWI service.

Command Default

Voice-mail server settings are disabled by default.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Using the **mwi-server** command a user can request that the UA subscribe to a voice-mail server requesting notification of mailbox status. When there is a status change, the voice-mail server notifies the UA. The UA then indicates to the user that there is a change in mailbox status with an MWI tone when the user takes the phone off-hook.

Only one voice-mail server can be configured per voice gateway. Use the **mwi-server** command with the **mwi** command to enable MWI functionality on the voice port. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. MWI status is always reset after a router reload.

Examples

The following example specifies voice-mail server settings on a voice gateway. The example includes the **unsolicited** keyword, enabling the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes.

```
sip-ua
 mwi-server dns:test.cisco.com expires 60 port 5060 transport udp unsolicited
```

For unsolicited Notify, the Contact header derives the voice-mail server address. If the unsolicited MWI message does not contain a Contact header, configure the voice-mail server on the gateway with the following special syntax to accept MWI Notify messages.

```
sip-ua
 mwi-server ipv4:255.255.255.255 unsolicited
```

Related Commands

Command	Description
mwi	Enables MWI for a specified voice port.
sip-us	Enables SIP UA configuration mode.
voice-port	Enters voice-port configuration mode.

Cisco IOS Voice Commands: N

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

name (dial peer cor custom)

To specify the name for a custom class of restrictions (COR), use the **name** command in dial peer COR custom configuration mode. To remove a specified COR, use the **no** form of this command.

name *class-name*

no name *class-name*

Syntax Description

class-name	Name that describes the specific COR.

Command Default

No default behavior or values.

Command Modes

Dial peer COR custom configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **dial-peer cor custom** and **name** commands define the names of capabilities on which to apply COR operation. Examples of names might include any of the following: call1900, call527, call9, or call 911. You must define the capabilities before you specify the COR rules.

You can define a maximum of 64 COR names.

Examples

The following example defines three COR names:

```
dial-peer cor custom
 name 900_call
 name 800_call
 name catchall
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named CORs apply to dial peers.

nat symmetric check-media-src

To enable the gateway, to check the media source of incoming Real-time Transport Protocol (RTP) packets in symmetric Network Address Translation (NAT) environments, use the **nat symmetric check-media-src** command in SIP user agent configuration mode. To disable media source checking, use the **no** form of this command.

nat symmetric check-media-src

no nat symmetric check-media-src

Syntax Description

This command has no arguments or keywords.

Command Default

Media source checking is disabled.

Command Modes

SIP user agent configuration (sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command provides the ability to enable or disable symmetric NAT settings for the Session Initiation Protocol (SIP) user agent. Use the **nat symmetric check-media-src** command to configure the gateway to check the media source address and port of the first incoming RTP packet. Checking for media packets is automatically enabled if the gateway receives the direction role “active or both”.

Examples

The following example enables checking the media source:

```
Router(config)# sip-ua
Router(config-sip-ua)# nat symmetric check-media-src
```

Related Commands

Command	Description
nat symmetric role	Defines endpoint settings to initiate or accept a connection for symmetric.

nat symmetric role

To define endpoint settings to initiate or accept a connection for symmetric Network Address Translation (NAT) configuration, use the **nat symmetric role** command in SIP user agent configuration mode. To disable the **nat symmetric role** configuration, use the **no** form of this command.

nat symmetric role {**active** | **passive**}

no nat symmetric role {**active** | **passive**}

Syntax Description

active	Sets the symmetric NAT endpoint role to active, originating an outgoing connection.
passive	Sets the symmetric NAT endpoint role to passive, accepting an incoming connection to the port number on the m=line of the Session Description Protocol (SDP) body sent from the SDP body to the other endpoint.

Command Default

The endpoint settings to initiate or accept connections for NAT configuration are not defined..

Command Modes

SIP user agent configuration (sip-ua)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command provides the ability to specify symmetric NAT endpoint settings for the SIP user agent. If the gateway does not receive the direction role, use the **nat symmetric role** command to define endpoint settings to initiate or accept a connection for symmetric NAT configuration. This is achieved by setting the symmetric NAT endpoint role to **active** or **passive**, respectively. Cisco recommends that you use the **nat symmetric role** command under the following conditions:

- Endpoints are aware of their presence inside or outside of NAT
- Endpoints parse and process direction:<role> in SDP

If the endpoints conditions are not satisfied, you may not achieve the desired results when you configure the **nat symmetric role** command.

Examples

The following example shows how to set the endpoint role in connection setup to active:

```
Router(config)# sip-ua
Router(config-sip-ua)# nat symmetric role active
```

Related Commands

Command	Description
nat symmetric check-media-src	Enables source media checking for symmetric NAT.

neighbor (annex g)

To configure the neighboring border elements (BEs) that interact with the local BE for the purpose of obtaining addressing information and aiding in address resolution, enter the **neighbor** command in Annex G configuration mode. To reset the default value, use the **no** form of this command.

neighbor *ip-address*

no neighbor

Syntax Description

ip-address	IP address of the neighbor that is used for exchanging Annex G messages.

Command Default

No default behavior or values

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example configures a neighboring BE that has an IP address and border element ID:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# neighbor 121.90.10.42
Router(config-annexg-neigh)# id be30
Router(config-annexg-neigh)# exit
```

Related Commands

Command	Description
advertise	Controls the types of descriptors that the BE advertises to its neighbors.
call-router	Enables the Annex G border element configuration commands.
id	Configures the local ID for the neighboring BE.

Command	Description
port	Configures the port number of the neighbor that is used for exchanging Annex G messages.
query-interval	Configures the interval at which the local BE will query the neighboring BE.

neighbor (tgrep)

To create a TGREP session with another device, use the **neighbor** command in TGREP configuration mode. To disable a TRIP connection, use the **no** form of this command.

neighbor *ip_address*

no neighbor *ip_address*

Syntax Description

ip_address	IP address of a peer device with which TGREP information will be exchanged.

Command Default No neighboring devices are defined

Command Modes TGREP configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples The following example shows that the gateway with the IP address 192.116.56.10 is defined as a neighbor for ITAD 1234:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# neighbor 192.116.56.10
```

Related Commands

Command	Description
tgrep local-itad	Enters TGREP configuration mode and defines an ITAD.

network-clock base-rate

To configure the network clock base rate for universal I/O serial ports 0 and 1, use the **network-clock base-rate** command in global configuration mode. To disable the current network clock base rate, use the **no** form of this command.

network-clock base-rate {**56k** | **64k**}

no network-clock base-rate {**56k** | **64k**}

Syntax Description

56k	Sets the network clock base rate to 56 kbps.
64k	Sets the network clock base rate to 64 kbps.

Command Default 56 kbps

Command Modes Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines This command applies to Voice over Frame Relay and Voice over ATM.

Examples The following example sets the network clock base rate to 64 kbps:

```
network-clock base-rate 64k
```

Related Commands

Command	Description
network-clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.
network-clock-switch	Configures the switch delay time to the next priority network clock source when the current network clock source fails.

network-clock-participate

To allow the ports on a specified network module or voice/WAN interface card (VWIC) to use the network clock for timing, use the **network-clock-participate** command in global configuration mode. To restrict the device to use only its own clock signals, use the **no** form of this command.

network-clock-participate [**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*]

no network-clock-participate [**nm** *slot* | **wic** *wic-slot*]

Syntax Description

slot *slot-number*	(Optional) Network module slot number on the router chassis. Valid values are from 1 to 6.
wic *wic-slot*	Configures the WAN interface card (WIC) slot number on the router chassis. Valid values are 0 or 1.
aim *aim-slot-number*	Configures the Advanced Integration Module (AIM) in the specified slot. The *aim-slot-number* values are 0 or 1 for the Cisco 3660 and 0 or 1 for the Cisco 3725, and Cisco 3745.

Command Default

No network clocking is enabled, and interfaces are restricted to using the clocking generated on their own modules.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 3660.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	The **slot** keyword was replaced by the **nm** keyword and the **wic** keyword and the *wic-slot* argument were added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T with support for the Cisco 3660, Cisco 3725, and Cisco 3745. Clocks can be synchronized on two ports. The **aim** keyword was added. The **nm** keyword was replaced by the **slot** keyword.
12.4(15)T9	This command was integrated into Cisco IOS Release 12.4(15)T9, and support was added for the NM-CEM-4SER modules.

Usage Guidelines

This command is used for ATM segmentation and reassembly or digital signal processing and Cisco 3660, Cisco 3725, and Cisco 3745 routers.

This command applies to any network module with T1/E1 controllers to provide clocks from a central source (MIX module for the Cisco 3660) to the network module and to the port on the network module. Then that port can be selected as the clock source with the **network-clock-select** command to supply clock to other ports or network modules that choose to participate in network clocking with the **network-clock-participate** command. This command synchronizes the clocks for two ports.

On the Cisco 3700 series, you must use the **network-clock-participate** command and either the **wic** *wic-slot* keyword and argument or the **slot** *slot-number* keyword and argument.

Note If the AIM takes its clock signals from a T1 or E1 controller, it is mandatory to use the **network-clock-select** and **network-clock-participate** commands for ATM. The clocks for the ATM and voice interfaces do not need to be synchronous, but improved voice quality may result if they are.

Note The only VWICs that can participate in network clocking are digital T1/E1 packet voice trunk network modules (NM-HDV), and Fast Ethernet network modules (NM-2W, NM-1FE. and NM-2FE).

Note Beginning with Cisco IOS Release 12.4(15)T9, the **network-clock-participate** command can also be used for the NM-CEM-4SER modules. When the **network-clock-participate** command is configured, the clock is derived from the backplane. When the **no network-clock-participate** command is configured, the local oscillator clock is used.

Examples

The following example configures the network module in slot 5 to participate in network clocking on a Cisco 3660 with a MIX module:

```
network-clock-participate slot 5
network-clock-select 1 e1
```

The following example on a Cisco 3700 series router specifies that the AIM participates in network clocking and selects port E1 0/1 to provide the clock signals.

```
Router(config)# network-clock-participate wic 0
Router(config)# network-clock-participate aim 0
Router(config)# network-clock-select 2 E1 0/1
```

The following example on a Cisco 3660 specifies the slot number that participates in network clocking and selects port E1 5/0:

```
Router(config)# network-clock-participate slot 5
Router(config)# network-clock-select 1 E1 5/0
```

Related Commands

Command	Description
network-clock-select	Specifies selection priority for the clock sources.
network-clock-source	Selects the port to be the clock source to supply clock resources to other ports or network modules.

network-clock-select

To name a source to provide timing for the network clock and to specify the selection priority for this clock source, use the **network-clock-select** command in global configuration mode. To cancel the network clock selection, use the **no** form of this command.

network-clock-select *priority* {**bri** | **atm** | **t1** | **e1**} *slot/port*

no network-clock-select *priority* {**bri** | **atm** | **t1** | **e1**} *slot/port*

Syntax Description

priority	Selection priority for the clock source (1 is the highest priority). The clock with the highest priority is selected to drive the system time-division-multiplexing (TDM) clocks. When the higher-priority clock source fails, the next-higher-priority clock source is selected. Ranges are as follows: • Cisco 2600 series: 1 to 4 • Cisco 3660: 1 to 8 • Cisco 2800 series: 1 to 8
bri	Specifies that the slot is configured as BRI.
atm	Specifies that the slot is configured as ATM.
t1	Specifies that the slot is configured as T1.
e1	Specifies that the slot is configured as E1.
slot	Slot number identifying the controller that is the clock source. • Cisco 2600 series or Cisco 2600XM—0 (built-in WIC slot) or 1 (network module slot). • Cisco 3660, Cisco 3725, and Cisco 3745—1 to 6. • Cisco 2800 series—0, 1, or 2.
port	Port number identifying the controller that is the clock source. The range is from 0 to 3. For the Cisco 2800 series, the range is 0 to 7 (for example, BRI interface can be 2/0 to 2/7).
serial 0	(Optional) Specifies serial interface 0 as the clock source. This option is not available on the Cisco 2800 series or Cisco 3800 series.
system	(Optional) Specifies the system clock as the clock source. This option is not available on the Cisco 2800 series or Cisco 3800 series.
bvm	Clocking priority for the BRI voice module (BVM). This option is not available on the Cisco 2800 series or Cisco 3800 series.
controller	(Optional) Specifies which controller is the clock source. You can specify either the trunk controller (T1/E1 0) or the digital voice module (T1/E1 1). This option is not available on the Cisco 2800 series or Cisco 3800 series.

Command Default

Cisco 2600 series and Cisco 2600XM

The network clock source is the Advanced Integration Module (AIM) phase-locked loop (PLL) with priority 5, which indicates that the network clock is in free running mode.

Cisco 3660, Cisco 3725, and Cisco 3745

The network clock source is the backplane PLL with priority 9, which indicates that the network clock is in free running mode.

Note Default clock values can fall outside the configurable range because they are derived from an external source.

Command Modes

Global configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.0(3)XG	The BVM as a possible network clock source was added.
12.1(5)XM	This command was implemented on the Cisco 3660. The keywords **t1** and **e1** were introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	This command was implemented on the Cisco 2600 series and Cisco 3660 with AIMs installed.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 2691, Cisco 3725, and Cisco 3745.
12.3(8)T4	This command was integrated into Cisco IOS Release 12.3(8)T4 and the **bri** keyword was added. Support was also added for the Cisco 2800 series.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and the **atm** keyword was added. Support was also added for the Cisco 3800 series.

Usage Guidelines

When an active clock source fails, the system chooses the next lower priority clock source specified by this command. When a higher-priority clock becomes available, the system automatically reselects the higher-priority clock source.

Cisco 2600 series and Cisco 3660

This command is used on Cisco 2600 series and Cisco 2600XM with AIMs installed or on the Cisco 3660 with Multiservice Interchange (MIX) modules installed. This command names a controller to provide clocking signals to the backplane, which then provides the names to all the network modules that are participating in network clocking.

Examples

The following example shows how to select the controller in slot 5, port 1, to provide the clock at priority 3:

```
network-clock-select 3 t1 5/1
```

Related Commands

Command	Description
network-clock-participate	Configures a network module to participate in network clocking.
network-clock-switch	Configures the switch delay time to the next priority network clock source when the current network clock source fails or a higher priority clock source is up and available.
show network-clocks	Displays the network clock configuration and current primary clock source.

network-clock-switch

To configure the switch delay time to the next priority network clock source when the current network clock source fails, use the **network-clock-switch** command in global configuration mode. To cancel the network clock delay time selection, use the **no** form of this command.

network-clock-switch [*switch-delay* | **never**] [*restore-delay* | **never**]

no network-clock-switch

Syntax Description

switch-delay	(Optional) Delay time, in seconds, before the next-priority network clock source is used when the current network clock source fails. Range is from 0 to 99. Default is 10.
never	(Optional) No delay time before the current network clock source recovers.
restore-delay	(Optional) Delay time, in seconds, before the current network clock source recovers. Range is from 0 to 99.
never	(Optional) No delay time before the next-priority network clock source is used when the current network clock source fails.

Command Default

10 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example switches the network clock source after 20 seconds and sets the delay time before the current network clock source recovers to 20 seconds:

```
network-clock-switch 20 20
```

Related Commands

Command	Description
network-clock-select	Uses the network clock source to provide timing to the system backplane PCM bus.

non-linear

To enable nonlinear processing (NLP) in the echo canceller and set its threshold or comfort-noise attenuation, use the **non-linear** command in voice-port configuration mode. To disable nonlinear processing, use the **no** form of this command.

non-linear [**comfort-noise attenuation** {**0db | 3db | 6db | 9db**} | **threshold** *dB*]

no non-linear [**comfort-noise attenuation | threshold**]

Syntax Description

**0db	3db	6db	9db**	(Optional) Attenuation level of the comfort noise in dB. Default is **0db**, which means that comfort noise is not attenuated.
threshold *dB*	(Optional) Sets the threshold in dB. Range is -15 to -45. Default is -21. **Note** This keyword is not supported when using the extended G.168 echo canceller.

Command Default

NLP is enabled; comfort-noise attenuation is disabled; threshold is -21 dB.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.2(11)T	The **threshold** keyword was added.
12.2(13)T	This command was implemented on routers that support the extended G.168 echo canceller.
12.3(6)	The **comfort-noise** keyword was added.

Usage Guidelines

This command enables functionality that is also generally known as residual echo suppression. Use this command to shut off any signal if no near-end speech is detected. Enabling this command normally improves performance, although some users might perceive truncation of consonants at the end of sentences when this command is enabled.

Use the **comfort-noise** keyword if the comfort noise generated by the NLP sounds like hissing. Using this keyword makes the hissing sound less audible.

Note The **echo-cancel enable** command must be enabled for this command to take effect.

Examples

The following example enables nonlinear call processing on a Cisco 3600 series router:

```
voice-port 1/0/0
 non-linear
```

The following example sets the attenuation level to 9 dB on a Cisco 3600 series router:

```
voice-port 1/0/0
 non-linear comfort-noise attenuation 9db
```

Related Commands

Command	Description
echo-cancel enable	Enables echo cancellation for voice that is sent and received on the same interface.

notify (MGCP profile)

To specify the order in which automatic number identification (ANI) and dialed number identification service (DNIS) digits are reported to the Media Gateway Control Protocol (MGCP) call agent, use the **notify** command in MGCP profile configuration mode. To revert to the default, use the **no** form of this command.

notify {**ani-dnis** | **dnis-ani**}

no notify {**ani-dnis** | **dnis-ani**}

Syntax Description

ani-dnis	ANI digits are sent in the first notify message, followed by DNIS. This is the default.
dnis-ani	DNIS digits are sent in the first notify message, followed by ANI.

Command Default

The default order is ANI first and DNIS second.

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command controls the order of ANI and DNIS when using the Feature Group D (FGD) Exchange Access North American (EANA) protocol on a T1 interface. Selecting the **ani-dnis** keyword causes the ANI digits to be sent in the first NTFY message to the MGCP call agent and the DNIS digits to be sent in a second NTFY message. Selecting the **dnis-ani** keyword causes the DNIS digits to be sent in the first NTFY message to the MGCP call agent and the ANI digits to be sent in a second NTFY message.

Examples

The following example sets the digit order to DNIS first and ANI second for the default MGCP profile:

```
Router(config)# mgcp profile default
Router(config-mgcp-profile)# notify dnis-ani
```

Related Commands

Command	Description
mgcp package-capability	Specifies an MGCP package capability type for a media gateway.
mgcp profile	Defines an MGCP profile to be associated with one or more MGCP endpoints
show mgcp	Displays MGCP configuration information.
show mgcp profile	Displays information for MGCP profiles.

notify redirect

To enable application handling of redirect requests for all VoIP dial peers on a Cisco IOS voice gateway, use the **notify redirect** command in voice service VoIP configuration mode. To disable application handling of redirect requests on the gateway, use the **no** form of this command. To return the gateway to the default **notify redirect** command settings, use the **default** form of this command.

notify redirect {**ip2ip** | **ip2pots**}

no notify redirect {**ip2ip** | **ip2pots**}

default notify redirect {**ip2ip** | **ip2pots**}

Syntax Description

ip2ip	Enables notify redirection for IP-to-IP calls.
ip2pots	Enables notify redirection for IP-to-IP calls for IP-to-POTS calls.

Command Default

Notify redirection for IP-to-IP calls is enabled.
Notify redirection for IP-to-POTS calls is disabled.
Notify redirection for Session Initiation Protocol (SIP) phones registered to Cisco Unified Communications Manager Express (Cisco Unified CME) is enabled.

Command Modes

Voice service VoIP configuration (conf-voi-serv)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use this command to enable notify redirection globally on a gateway. Use the **notify redirect** command in dial peer voice configuration mode to configure notify redirection settings for IP-to-IPand IP-to-POTS calls on a specific inbound dial peer on a gateway.

Note This command is supported on Cisco Unified Communications Manager Express (Cisco Unified CME), release 3.4 and later releases and on Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) release 3.4 and later releases. However, to use the **notify redirect** command in voice service VoIP configuration mode on compatible Cisco Unified SIP SRST devices, you must first use the **allow-connections** command to enable the corresponding call flows on the SRST gateway.

Examples

The following is partial sample output from the **show running-config** command showing that notify redirection has been set up globally for both IP-to-IP and IP-to-POTS calling (because support of IP-to-IP calls is enabled by default, the ip2ip setting does not appear in the output).

```
voice service voip
```

```
notify redirect ip2pots
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to sip
no supplementary-service h450.2
no supplementary-service h450.3
sip
registrar server expires max 600 min 60
```

Related Commands

Command	Description
allow-connections	Allows connections between specific endpoint types in a VoIP network.
notify redirect (dial peer)	Enables application handling of redirect requests on a specific VoIP dial peer on a Cisco IOS voice gateway.

notify redirect (dial peer)

To enable application handling of redirect requests on a specific VoIP dial peer on a Cisco IOS voice gateway, use the **notify redirect** command in dial peer voice configuration mode. To disable notify redirection on the gateway, use the **no** form of this command. To return the gateway to the default notify redirection settings, use the **default** form of this command.

notify redirect {**ip2ip** | **ip2pots**}

no notify redirect {**ip2ip** | **ip2pots**}

default notify redirect {**ip2ip** | **ip2pots**}

Syntax Description

ip2ip	Enables notify redirect for IP-to-IP calls.
ip2pots	Enables notify redirect for IP-to-POTS calls.

Command Default

Notify redirection for IP-to-IP is enabled.
Notify redirection for IP-to-POTS is disabled.
Notify redirection for Session Initiation Protocol (SIP) phones registered to Cisco Unified Communications Manager Express (Cisco Unified CME) is enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use this command in dial peer configuration mode to configure IP-to-IP and IP-to-POTS calls on an inbound dial peer on a Cisco IOS voice gateway. This command configures notify redirection settings on a per-dial-peer basis.

When notify redirect is enabled in dial peer voice configuration mode, the configuration for the specific dial peer is activated only if the dial peer is an inbound dial peer. To enable notify redirect globally on a Cisco IOS voice gateway, use the **notify redirect** command in voice service VoIP configuration mode.

Note This command is supported on Cisco Unified Communications Manager Express (Cisco Unified CME), release 3.4 and later releases and Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) release 3.4 and later releases. However, to use the **notify redirect** command in voice service VoIP configuration mode on compatible Cisco Unified SIP SRST devices, you must first use the **allow-connections** command to enable the corresponding call flows on the SRST gateway.

Examples

The following is partial sample output from the **show running-config** command showing that notify redirection is enabled for both IP-to-IP and IP-to-POTS calls on VoIP dial peer 8000 (because support of IP-to-IP calls is enabled by default, the ip2ip setting does not appear in the output):

```
dial-peer voice 8000 voip
 destination-pattern 80..
 notify redirect ip2pots
 session protocol sipv2
 session target ipv4:209.165.201.15
 dtmf-relay rtp-nte
 codec g711ulaw
!
```

Related Commands

Command	Description
allow-connections	Allows connections between specific endpoint types in a VoIP network.
notify redirect	Enables application handling of redirect requests for all VoIP dial peers on a Cisco IOS voice gateway.

notify telephone-event

To configure the maximum interval between two consecutive NOTIFY messages for a particular telephone event, use the **notify telephone-event** command in SIP UA configuration mode. To reset the interval to the default value, use the **no** form of this command.

notify telephone-event max-duration *milliseconds*

no notify telephone-event

Syntax Description

max-duration *milliseconds*	Time interval between consecutive NOTIFY messages for a single DTMF event, in milliseconds. Range is from 40 to 3000. Default is 2000.

Command Default

2000 milliseconds

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was modified. The acceptable value range for the *milliseconds* argument was expanded (the lower end of the range was changed from 500 to 40).
12.4(24)T3	This command was modified. The acceptable value range for the *milliseconds* argument was expanded (the lower end of the range was changed from 500 to 40).

Usage Guidelines

The **notify telephone-event** command works with the **dtmf-relay sip-notify** command. The **dtmf-relay sip-notify** command forwards out-of-band DTMF tones by using SIP NOTIFY messages. The **notify telephone-event** command sets the maximum time interval between consecutive NOTIFY messages for a single DTMF event. The maximum time is negotiated between two SIP endpoints and the lowest duration value is the one selected. This duration is negotiated during call establishment as part of negotiating the SIP-NOTIFY DTMF relay.

The originating gateway sends an indication of DTMF relay in an Invite message using the SIP Call-Info header. The terminating gateway acknowledges the message with an 18x/200 Response message, also using the Call-Info header. The set duration appears in the Call-Info header in the following way:

```
Call-Info: <sip: address>; method="Notify;Event=telephone-event;Duration=msec"
```

For example, if the maximum duration of gateway A is set to 1000 ms, and gateway B is set to 700 ms, the resulting negotiated duration would be 700 ms. Both A and B would use the value 700 in all of their NOTIFY messages for DTMF events.

Examples

The following example sets the maximum duration for a DTMF event to 40 ms.

```
Router(config)# sip-ua
Router(config-sip-ua)# notify telephone-event max-duration 40
```

Related Commands

Command	Description
dtmf-relay sip-notify	Forwards DTMF tones using SIP NOTIFY messages.

nsap

To specify the network service access point (NSAP) address for a local video dial peer, use the **nsap** command in dial peer configuration mode. To remove any configured NSAP address from the dial peer, use the **no** form of this command.

nsap *nsap-address*

no nsap

Syntax Description

nsap-address	A 40-digit hexadecimal number; the number must be unique on the device.

Command Default No NSAP address for a video dial peer is configured

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(9)T.

Usage Guidelines The address must be unique on the router.

Examples The following example sets up an NSAP address for the local video dial peer designated as 10:

```
dial-peer video 10 videocodec
 nsap 47.0091810000000002F26D4901.333333333332.02
```

Related Commands

Command	Description
dial-peer video	Defines a video ATM dial peer for a local or remote video codec, specifies video-related encapsulation, and enters dial peer configuration mode.
show dial-peer video	Displays dial peer configuration.

null-called-number

To substitute a user-defined number as the called number IE when an incoming H.323 setup message does not contain a called number IE, use the **null-called-number** command in voice service H.323 configuration mode. To disable the addition of the number used as the called number IE, use the **no** form of this command.

null-called-number override *string*

no null-called-number

Syntax Description

override *string*	Specifies the user-defined series of digits for the E.164 or private dialing plan telephone number when the called number IE is missing from the H.323 setup message. Valid entries are the digits 0 through 9.

Command Default

The command behavior is disabled. H.323 setup messages missing the called number IE are disconnected.

Command Modes

Voice service h323 configuration (conf-serv-h323)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

For a call connection to be completed the incoming H.323 setup messages must include the called number IE and the E.164 destination address. Calls lacking called number IE are disconnected. The null-called-number is a user-defined number used when the called number IE is missing to complete the call.

Examples

The following example shows the number 4567 configured as the user-defined number used to complete a call when the H.323 setup message is missing the called number IE:

```
Router(conf-serv-h323)# null-called-number override 4567
```

numbering-type

To match on a number type for a dial-peer call leg, use the **numbering-type** command in dial peer configuration mode. To remove the numbering type for a dial-peer call leg, use the **no** form of this command.

numbering-type {**international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown**}

no numbering-type {**international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown**}

Syntax Description

international	International numbering type.
abbreviated	Abbreviated numbering type.
national	National numbering type.
network	Network numbering type.
reserved	Reserved numbering type.
subscriber	Subscriber numbering type.
unknown	Numbering type unknown.

Command Default

No default behaviors or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced on the Cisco AS5300.
12.0(7)XK	This command was implemented as follows: • VoIP: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoFR: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoATM: Cisco 3600 series, Cisco MC3810
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented as follows: • VoIP: Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, Cisco 7500 series
12.1(2)T	This command was implemented as follows: • VoIP: Cisco MC3810 • VoFR: Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • VoATM: Cisco 3600 series, Cisco MC3810
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command is supported for POTS, VoIP, VoFR, and VoATM dial peers. The numbering type options are implemented as defined by the ITU Q.931 specification.

Examples

The following example shows how to configure a POTS dial peer for network usage:

```
dial-peer voice 100 pots
 numbering-type network
```

The following example shows how to configure a VoIP dial peer for subscriber usage:

```
dial-peer voice 200 voip
 numbering-type subscriber
```

Related Commands

Command	Description
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

num-exp

To define how to expand a telephone extension number into a particular destination pattern, use the **num-exp** command in global configuration mode. To remove the configured number expansion, use the **no** form of this command.

num-exp *extension-number expanded-number*

no num-exp *extension-number*

Syntax Description

extension-number	One or more digits that define an extension number for a particular dial peer.
expanded-number	One or more digits that define the expanded telephone number or destination pattern for the extension number listed.

Command Default No number expansion is defined.

Command Modes Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(4)XL	This command was implemented on the Cisco AS5800.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was modified. It was integraged into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use this command to define how to expand a particular set of numbers (for example, a telephone extension number) into a particular destination pattern. With this command, you can bind specific extensions and expanded numbers together by explicitly defining each number, or you can define extensions and expanded numbers using variables. You can also use this command to convert seven-digit numbers to numbers containing fewer than seven digits.

You can configure a maximum of 250 number extensions before the router sends an error message stating that the limit has been reached.

Use a period (.) as a variable or wildcard, representing a single number. Use a separate period for each number that you want to represent with a wildcard—for example, if you want to replace four numbers in an extension with wildcards, type in four periods.

Examples

The following example expands the extension number 50145 to the number 14085550145:

```
num-exp 50145 14085550145
```

The following example expands all five-digit extensions beginning with 5 such that the 5 is replaced with the digits 1408555 at the beginning of the extension number:

```
num-exp 5.... 1408555....
```

Related Commands

Command	Description
dial-peer terminator	Designates a special character to be used as a terminator for variable length dialed numbers.
forward-digits	Specifies which digits to forward for voice calls.
prefix	Specifies a prefix for a dial peer.

Cisco IOS Voice Commands: O

This chapter contains the commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

offer call-hold

To specify globally how the Session Initiation Protocol (SIP) gateway should initiate call-hold requests, use the **offer call-hold** command in SIP user-agent configuration mode. To disable a method of initiating call hold, use the **no** form of this command.

offer call-hold {**conn-addr** | **direction-attr**}

no offer call-hold {**conn-addr** | **direction-attr**}

Syntax Description

conn-addr	Specifies the RFC 2543 method of using the connection address for initiating call-hold requests. The RFC 2543 method uses 0.0.0.0.
direction-attr	Specifies the current RFC 3264 method of using the direction attribute (a=sendonly) for initiating call-hold requests.

Command Default **direction-attr**

Command Modes SIP user-agent configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines Cisco SIP gateways support receiving call-hold requests in either of the two formats, but the direction attribute is recommended. Specifying a call-hold format is only available globally with the **offer call-hold** command; configuration is not available at the dial-peer level.

Examples The following example initiates call hold by configuring the gateway to send a=sendonly in the Session Description Protocol (SDP). Using the **direction-attr** keyword is the current and preferred method to initiate call hold.

```
sip-ua
 retry invite 3
 offer call-hold direction-attr
```

The following example initiates call hold by configuring the gateway to send 0.0.0.0 as the IP address in the c=line.

```
sip-ua
 retry invite 3
 offer call-hold conn-addr
```

Related Commands

Command	Description
show sip-ua status	Displays status for the SIP UA.
suspend-resume	Enables SIP Suspend and Resume functionality.

operation

To select a specific cabling scheme for E&M ports, use the **operation** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

operation {**2-wire** | **4-wire**}

no operation {**2-wire** | **4-wire**}

Syntax Description

2-wire	Two-wire E&M cabling scheme.
4-wire	Four-wire E&M cabling scheme.

Command Default

2-wire E&M cabling scheme

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.

Usage Guidelines

This command affects only voice traffic. Signaling is independent of 2-wire versus 4-wire settings. If the wrong cable scheme is specified, the user might get voice traffic in only one direction.

Using this command on a voice port changes the operation of both voice ports on a VPM card. The voice port must be shut down and then opened again for the new value to take effect.

This command is not applicable to FXS or FXO interfaces because they are, by definition, 2-wire interfaces.

Examples

The following example specifies that an E&M port uses a 4-wire cabling scheme:

```
voice-port 1/0/0
 operation 4-wire
```

The following example specifies that an E&M port uses a 2-wire cabling scheme:

```
voice-port 1/1
 operation 2-wire
```

options-ping

To enable in-dialog OPTIONS, use the **options-ping** command in global configuration mode. To disable, use the **no** form of this command.

options-ping *seconds*

no options-ping *seconds*

Syntax Description

seconds	Intervals, in seconds OPTIONS transactions are sent. Range is 60-1200, there is no default.

Command Default This command is disabled by default.

Command Modes Global

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines The in-dialog OPTIONS refresh command eanbles an alterante refresh mechanism to RTP/RTCP media inactivity timer and session timer can be used on SIP-to-SIP and SIP-to-H.323 calls. The refresh with in-dialog OPTIONS method is meant to only be hop-to-hop, and not end-to-end. Since session timer achieves similar results, the OPTIONs refresh/ping will not take affect when session timer is negotiated. The behavior on the H.323 endpoint is as if it was a TDM-SIP call. The generating in-dialog OPTIONS is enabled at the global level or dialpeer level. The system default setting is disabled. This feature can be use by both a TDM voice gateway and an IP-to-IP gateway.

Examples The following example sets the in-dialog refresh time to 60 seconds:

```
Router(conf-serv-sip)# options-ping 60
```

Related Commands

Command	Description
options-ping	Enables in-dialog OPTIONS at the global level.
options-ping (dial peer)	Enables in-dialog OPTIONS on a dial-peer.

options-ping (dial peer)

To enable in-dialog OPTIONS, use the **options-ping** command in global configuration mode. To disable, use the **no** form of this command.

options-ping *seconds*

no options-ping *seconds*

Syntax Description

seconds	Intervals, in seconds OPTIONS transactions are sent. Range is 60-1200, there is no default.

Command Default

This command is disabled by default.

Command Modes

dial peer configuration mode

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The in-dialog OPTIONS refresh command eanbles an alterante refresh mechanism to RTP/RTCP media inactivity timer and session timer can be used on SIP-to-SIP and SIP-to-H.323 calls. The refresh with in-dialog OPTIONS method is meant to only be hop-to-hop, and not end-to-end. Since session timer achieves similar results, the OPTIONs refresh/ping will not take affect when session timer is negotiated. The behavior on the H.323 endpoint is as if it was a TDM-SIP call. The generating in-dialog OPTIONS is enabled at the global level or dialpeer level. The system default setting is disabled. This feature can be use by both a TDM voice gateway and an IP-to-IP gateway.

Examples

The following example sets the in-dialog refresh time to 60 seconds:

```
Router(conf-serv-sip)# options-ping 60
```

Related Commands

Command	Description
options-ping	Enables in-dialog OPTIONS at the global level.
options-ping (dial peer)	Enables in-dialog OPTIONS on a dial-peer.

outbound-proxy

To configure a Session Initiation Protocol (SIP) outbound proxy for outgoing SIP messages globally on a Cisco IOS voice gateway, use the **outbound-proxy** command in voice service SIP configuration mode. To globally disable forwarding of SIP messages to a SIP outbound proxy globally, use the **no** form of this command.

outbound-proxy {**dhcp** | **ipv4:***ip-address*[**:***port-number*] | **dns:***host***:***domain* [**reuse**]}

no outbound-proxy

Syntax Description

dhcp	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to the SIP server obtained via DHCP.
ipv4:*ip-address*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all SIP dialog-initiating requests are sent to this IP address. The colon is required.
:*port-number*	(Optional) The port to which all SIP dialog-initiating requests are sent at the specified IP address. Port number ranges from 0 to 65535. The default is 5060. The colon is required.
dns:*host***:***domain*	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway; all initiating requests are sent to the specified destination domain. The colon is required.
reuse	(Optional) Reuses the outbound proxy address established during registration for all subsequent registration refreshes and calls.

Command Default

The Cisco IOS voice gateway does not forward outbound SIP messages to a proxy.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.
12.4(22)YB	This command was modifed. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **reuse** keyword was added.

Usage Guidelines

You can use the **outbound-proxy** command in voice service SIP configuration mode to specify outbound proxy settings globally for a Cisco IOS voice gateway. You can also use the **voice-class sip outbound-proxy** command in dial peer voice configuration mode to configure settings for an individual dial peer that override or defer to the global settings for the gateway. However, if both a Cisco Unified Communications Manager Express (CME) and a SIP gateway are configured on the same router, then there is a scenario that can cause incoming SIP messages from line-side phones to be confused with SIP

messages coming from the network side. To avoid failed calls caused by this scenario, disable the SIP outbound proxy setting for all line-side phones on a dial peer using the **outbound-proxy system** command in voice register global configuration mode.

Examples

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using an IP address:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy ipv4:10.1.1.1
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using a destination hostname and domain:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dns:sipproxy:example.com
```

The following example shows how to specify the SIP outbound proxy globally for a Cisco IOS voice gateway using the DHCP protocol:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# outbound-proxy dhcp
```

Related Commands

Command	Description
outbound-proxy system	Specifies whether Cisco Unified CME line-side SIP phones use the outbound proxy settings configured globally for a Cisco IOS voice gateway.
voice-class sip outbound-proxy	Configures SIP outbound proxy settings for an individual dial peer that override global settings for the Cisco IOS voice gateway.

outbound retry-interval

To define the retry period for attempting to establish the outbound relationship between border elements, use the **outbound retry-interval** command in Annex G neighbor service configuration mode. To disable the command, use the **no** form of this command.

outbound retry-interval *interval*

no outbound retry-interval

Syntax Description

interval	Amount of time, in seconds, to establish the outbound relationship. Range is from 1 to 2147483. The default is 30.

Defaults

30 seconds

Command Modes

Annex G neighbor service configuration (config-nxg-neigh-svc)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Service relationships are defined to be unidirectional. When a service relationship is established between border element A and border element B, A is entitled to send requests to B and expect responses. For B to send requests to A and expect responses, a second service relationship must be established. From A's perspective, the service relationship it establishes with B is designated as the "outbound" service relationship.

Use this command to set the retry period for attempting to bring up the outbound relationship between border elements.

Examples

The following example shows how to set the retry interval to 300 seconds (5 minutes):

```
Router(config-nxg-neigh-svc)# outbound retry-interval 300
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time that a border element will attempt delivery.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.

outgoing called-number

To configure debug filtering for outgoing called numbers, use the **outgoing called-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing called-number *string*

no outgoing called-number *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range. • Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.

Defaults

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The outgoing called number goes out after number translation and expansion.

Examples

The following example shows the voice call debug filter set to match outgoing called number 8288807:

```
call filter match-list 1 voice
 outgoing called-number 8288807
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

outgoing calling-number

To configure debug filtering for outgoing calling numbers, use the **outgoing calling-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing calling-number *string*

no outgoing calling-number *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range. • Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.

Defaults

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The outgoing calling number goes out after number translation and expansion.

Examples

The following example shows the voice call debug filter set to match outgoing calling number 8288807:

```
call filter match-list 1 voice
 outgoing calling-number 8288807
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

outgoing dialpeer

To configure debug filtering for the outgoing dial peer, use the **outgoing dialpeer** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing dialpeer *tag*

no outgoing dialpeer *tag*

Syntax Description

tag	Digits that identify a specific dial peer. Valid entries are 1 to 2,147,483,647.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing dial peer 12:

```
call filter match-list 1 voice
 outgoing dialpeer 12
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming port	Configure debug filtering for the incoming port.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing media local ipv4

To configure debug filtering for the outgoing media local IPv4 addresses for the voice gateway receiving the media stream, use the **outgoing media local ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing media local ipv4 *ip_address*

no outgoing media local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match outgoing media on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing media local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing media remote ipv4

To configure debug filtering for the outgoing media remote IPv4 addresses for the voice gateway receiving the media stream, use the **outgoing media remote ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing media remote ipv4 *ip_address*

no outgoing media remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match outgoing media on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing media remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

outgoing port

To configure debug filtering for the outgoing port, use the **outgoing port** command in call filter match list configuration mode. To disable, use the **no** form of this command.

Cisco 2600, Cisco 3600, and Cisco 3700 Series

outgoing port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

no outgoing port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

Cisco 2600 and Cisco 3600 Series with a High-Density Analog Network Module (NM-HDA)

outgoing port {*slot-number*/*subunit-number*/*port*}

no outgoing port {*slot-number*/*subunit-number*/*port*}

Cisco AS5300

outgoing port *controller-number*:**D**

no outgoing port *controller-number*:**D**

Cisco AS5400

outgoing port *card/port*:**D**

no outgoing port *card/port*:**D**

Cisco AS5800

outgoing port {*shelf*/*slot*/*port*:**D** | *shelf*/*slot*/*parent*:*port*:**D**}

no outgoing port {*shelf*/*slot*/*port*:**D** | *shelf*/*slot*/*parent*:*port*:**D**}

Cisco MC3810

outgoing port *slot*/*port*

no outgoing port *slot*/*port*

Syntax Description

Cisco 2600, Cisco 3600 and Cisco 3700 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
port	Voice port number. Valid entries are 0 and 1.
slot	The router location in which the voice port adapter is installed. Valid entries are 0 to 3.

port:	Indicates the voice interface card location. Valid entries are 0 and 3.
ds0-group-no	Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300

controller-number	T1 or E1 controller.
:D	D channel associated with ISDN PRI.

Cisco AS5400

card	Specifies the T1 or E1 card. Valid entries for the *card* argument are 1 to 7.
port	Specifies the voice port number. Valid entries are 0 to 7.
:D	Indicates the D channel associated with ISDN PRI.

Cisco AS5800

shelf	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *shelf* argument are 0 to 9999.
slot	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *slot* argument are 0 to 11.
port	Specifies the voice port number. • T1 or E1 controller on the T1 card —Valid entries are 0 to 11. • T1 controller on the T3 card—Valid entries are 1 to 28
:*port*	Specifies the value for the *parent* argument. The only valid entry is 0.
:D	Indicates the D channel associated with ISDN PRI.

Cisco MC3810

slot	The *slot* argument specifies the number slot in the router in which the VIC is installed. The only valid entry is 1.
port	The *port* variable specifies the voice port number. Valid interface ranges are as follows: • T1—ANSI T1.403 (1989), Telcordia TR-54016. • E1— ITU G.703. • Analog voice—Up to six ports (FXS, FXO, E & M). • Digital voice— Single T1/E1 with cross-connect drop and insert, CAS and CCS signaling, PRI QSIG. • Ethernet—Single 10BASE-T. • Serial—Two five-in-one synchronous serial (ANSI EIA/TIA-530, EIA/TIA-232, EIA/TIA-449; ITU V.35, X.21, Bisync, Polled async).

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match outgoing port 1/1/1 on a Cisco 3660 voice gateway:

```
call filter match-list 1 voice
 outgoing port 1/1/1
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
show call filter match-list	Display call filter match lists.

outgoing signaling local ipv4

To configure debug filtering for the outgoing signaling local IPv4 addresses for the gatekeeper managing the signaling, use the **outgoing signaling local ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing signaling local ipv4 *ip_address*

no outgoing signaling local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match outgoing signaling on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing signaling local ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

outgoing signaling remote ipv4

To configure debug filtering for the outgoing signaling remote IPv4 addresses for the gatekeeper managing the signaling, use the **outgoing signaling remote ipv4** command in call filter match list configuration mode. To disable, use the **no** form of this command.

outgoing signaling remote ipv4 *ip_address*

no outgoing signaling remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match outgoing signaling on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 outgoing signaling remote ipv4 192.168.10.255
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
show call filter match-list	Display call filter match lists.

output attenuation

To configure a specific output attenuation value or enable automatic gain control, use the **output attenuation** command in voice-port configuration mode. To disable the selected output attenuation value, use the **no** form of this command.

output attenuation {*decibels* | **auto-control** [*auto-dbm*]}

no output attenuation {*decibels* | **auto-control** [*auto-dbm*]}

Syntax Description

decibels	Attenuation, in decibels (dB), at the transmit side of the interface. Range is integers from –27 to 16. The default is 0.
auto-control	Enable automatic gain control.
auto-dbm	(Optional) Target speech level, in decibels per milliwatt (dBm), to be achieved at the transmit side of the interface. Range is integers from –30 to 3. The default is –9.

Command Default

For Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and ear and mouth (E&M) ports: *decibels*: 0 decibels
auto-dbm: –9 dBm

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels* argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	The **auto-control** keyword and *auto-dbm* argument were added.

Usage Guidelines

A system-wide loss plan must be implemented using both the **input gain** and **output attenuation** commands. You must consider other equipment (including PBXs) in the system when creating a loss plan. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of –6 dB between phones. Connections are implemented to provide –6 dB of attenuation when the **input gain** and **output attenuation** commands are configured with the default value of 0 dB.

You cannot increase the gain of a signal to the public switched telephone network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or increasing the output attenuation.

You can increase the gain of a signal coming into the router. If the voice level is too low, you can increase the input gain by using the **input gain** command.

The **auto-control** keyword and *auto-dbm* argument are available on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). The **auto-control** keyword enables automatic gain control, which is performed by the digital signal processor (DSP). Automatic gain control adjusts speech to a comfortable volume when it becomes too loud or too soft. Because of radio network loss and other environmental factors, the speech level arriving at a router from an LMR system could be very low. You can use automatic gain control to ensure that the speech is played back at a more comfortable level. Because the gain is inserted digitally, the background noise can also be amplified. Automatic gain control is implemented as follows:

- Output level: –9 dB
- Gain range: –12 dB to 20 dB
- Attack time (low to high): 30 milliseconds
- Attack time (high to low): 8 seconds

Examples

On the Cisco 3600 series router, the following example configures a 3-dB loss to be inserted at the transmit side of the interface:

```
voice-port 1/0/0
 output attenuation 3
```

On the Cisco 3600 series router, the following example configures a 3-dB gain to be inserted at the transmit side of the interface:

```
voice-port 1/0/0
 output attenuation -3
```

On the Cisco AS5300, the following example configures a 3-dB loss to be inserted at the transmit side of the interface:

```
voice-port 0:D
 output attenuation 3
```

Related Commands

Command	Description
comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
echo-cancel enable	Enables the cancellation of voice that is sent out the interface and received back on the same interface.
input gain	Configures a specific input gain value or enables automatic gain control for a voice port.

Cisco IOS Voice Commands: P

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

package

To enter application-parameter configuration mode to load and configure a package, use the **package** command in application configuration mode. There is no **no** form of this command.

package *package-name location*

no package *package-name*

Syntax Description

package-name	Name that identifies the package.
location	Directory and filename of the package in URL format. For example, flash memory (flash:*filename*), a TFTP (tftp://../*filename*) or an HTTP server (http://../*filename*) are valid locations.

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to enter application parameter configuration mode to load and configure a package. A package is a linkable set of C or Tcl functions that provide functionality invoked by applications or other packages. They are not standalone. For example, a debit card application may use multiple language translation packages, such as English and French. These language translation packages can also be used by other applications without having to modify the package for each application using it.

The packages available on your system depend on the scripts, applications, and packages that you have installed. Your software comes with a set of built-in packages, and additional packages can be loaded using the Tcl **package** command. You can then use the **package** command in application configuration mode to access the parameters contained in those packages.

Examples The following example shows that a French language translation package is loaded:

```
Router(config-app)# package frlang http://server-1/language_translate.tcl
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specify the location of the Tcl or VoiceXML document to load for this application.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.

Command	Description
package language	Loads an external Tcl language module for use with an IVR application.
package session_xwork	Configure parameters in the built-in session_xwork package.

package appcommon

To configure parameters in the built-in common voice application package, use the **package appcommon** command in application configuration mode.

package appcommon

Syntax Description No arguments or keywords

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to configure common voice application package parameters. After you enter this command, use the **param** command to configure individual parameters.

Examples The following example shows using the **param security trusted** command to set the security level of a VoiceXML application to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
 package appcommon
 param security trusted
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package callsetup	Configures parameters in the built-in call setup package.
package language	Loads an external Tcl language module for use with an IVR application.
package session_xwork	Configure parameters in the built-in session_xwork package.

package callsetup

To configure parameters in the built-in call setup package, use the **package callsetup** command in application configuration mode. There is no **no** form of this command.

package callsetup

Command Default No arguments or keywords

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to configure parameters in the built-in call setup package. The callsetup package is used by applications and other packages to place outbound call legs and interwork them with incoming call legs. call setup After you enter this command, use the **param** command to configure individual parameters.

Examples

```
The following example shows the call transfer mode set to redirect:
application
 package callsetup
 param mode redirect
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package language	Loads an external Tcl language module for use with an IVR application.
package session_xwork	Configure parameters in the built-in session_xwork package.

package language

To load an external Tool Command Language (Tcl) language module for use with an interactive voice response (IVR) application, use the **package language command in** application configuration mode. There is no **no** form of the command.

package language *prefix url*

Syntax Description

prefix	Two-character prefix for the language; for example, "*en*" for English or "*ru*" for Russian.
url	Location of the module.

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call language voice** command.

Usage Guidelines Use this command to load language packages for use by applications or other packages. The built-in languages are English (*en)*, Chinese (*ch)*, and Spanish (*sp)*. If you specify "*en*", "*ch*", or "*sp*", the new Tcl module replaces the built-in language functionality. When you add a new Tcl module, you create your own prefix to identify the language. When you configure and load the new languages, any upper-layer application (Tcl IVR) can use the language.

After loading language packages, you can configure an application or other package to use the new language package using the **param language** or **paramspace language location** command.

Examples The following example adds Russian (*ru*) as a Tcl module and configures the debitcard application to use Russian for prompts:

```
application
package language ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
service debitcard tftp://server-1/tftpboot/scripts/app_debitcard.2.0.2.8.tcl
param language ru
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.

Command	Description
package session_xwork	Configures parameters in the built-in session_xwork package.
param language	Configures the language parameter in a service or package on the gateway.
paramspace language location	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

package persistent

To configure the package type used when reporting persistent events for a multifrequency (MF) tone channel-associated signaling (CAS) endpoint type using a specific Media Gateway Control Protocol (MGCP) profile, use the **package persistent** command in MGCP profile configuration mode. To disable the persistent status, use the **no** form of this command.

package persistent *package-name*

no package persistent *package-name*

Syntax Description

package-name	Package name. Valid names are ms-package and mt-package.

Command Default ms-package

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a MGCP profile.

This command is used only with MF trunks (gateway voice ports configured with the **dial-type mf** command in voice-port configuration mode). Because the same persistent event can be defined in different MGCP packages, you may need to use this command to tell the gateway which package to use when reporting persistent events to the call agent for the endpoints in this MGCP profile. For example, a T1 may be configured as an MF trunk, but there is more than one MGCP package that applies to an MF trunk. An *ans* (call answer) event must be mapped to the appropriate package for call-agent notification. This command allows different T1s to be configured for different CAS protocols.

The MS package is used with certain PBX direct inward dial (DID) and direct outward dial (DOD) trunks with wink-start or ground-start signaling as indicated in RFC 3064 (*MGCP CAS Packages*).

The MT package is a subset of the MS package, and it is used with certain operator services on terminating MF trunks on trunking gateway endpoints, as described in *PacketCable PSTN Gateway Call Signaling Protocol Specification* (TGCP) PKT-SP-TGCP-D02-991028, December 1, 1999.

Examples The following example enables event persistence for the MT package:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# package persistent mt-package
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure an MGCP profile associated with one or more endpoints or to configure the default profile.

package session_xwork

To configure parameters in the built-in session_xwork package, use the **package session_xwork** command in application configuration mode.

package session_xwork

Syntax Description No arguments or keywords

Command Default No default behavior or values

Command Default Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command to configure parameters in the built-in session x_work package. After you enter this command, use the **param** command to configure individual parameters.

For example, use this command with the **param default disc-prog-ind-at-connect** command to convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

Examples The following example shows how to configure the system to convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state:

```
application
 package session_xwork
 param default disc-prog-ind-at-connect
```

Related Commands

Command	Description
package	Enters application parameter configuration mode to load and configure a package.
package appcommon	Configures parameters in the built-in common voice application package.
package callsetup	Configures parameters in the built-in call setup package.
package language	Loads an external Tool Command Language (Tcl) language module for use with an interactive voice response (IVR) application.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.

param

To load and configure parameters in a package or a service (application) on the gateway, use the **param** command in application configuration mode. To reset a parameter to its default value, use the **no** form of this command.

param *param-name*

no param *param-name*

Syntax Description

param-name	Name of the parameter.

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command in application parameter configuration mode to configure parameters in a package or service. A package is a linkable set of C or Tcl functions that provide functionality invoked by applications or other packages. A service is a standalone application.

The parameters available for configuration differ depending on the package or service that is loaded on the gateway. The **param register** Tcl command in a service or package registers a parameter and provides a description and default values which allow the parameter to be configured using the CLI. The **param register** command is executed when the service or package is loaded or defined, along with commands such as **package provide**, which register the capability of the configured module and its associated scripts. You must configure and load the Tcl scripts for your service or package and load the package in order to configure its parameters. See the *Tcl IVR API Version 2.0 Programming Guide* for more information.

When a package or service is defined on the gateway, the parameters in that package or service become available for configuration when you use this command. Additional arguments and keywords are available for different parameters. To see a list of available parameters, enter **param ?**.

To avoid problems with applications or packages using the same parameter names, the *parameter namespace,* or *parameterspace* concept is introduced. When a service or a package is defined on the gateway, its parameter namespace is automatically defined. This is known as the service or package's local parameterspace, or "myparameterspace." When you use this command to configure a service or package's parameters, the parameters available for configuration are those contained in the local parameterspace. If you want to use parameter definitions found in different parameterspace, you can use the **paramspace** *parameter-namespace* command to map the package's parameters to a different parameterspace. This allows that package to use the parameter definitions found in the new parameterspace, in addition to its local parameterspace.

Examples

The following example shows how to configure a parameter in the httpios package:

```
application
 package httpios
 param paramA value4
```

Related Commands

Command	Description
call application voice	Defines the name of a voice application and specify the location of the Tcl or VoiceXML document to load for this application.
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
paramspace	Enables an application to use parameters from the local parameter space of another application.
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param access-method

To specify the access method for two-stage dialing for the designated application, use the **param access-method** command in application parameter configuration mode. To restore default values for this command, use the **no** form of this command.

param access-method {**prompt-user** | **redialer**}

no param access-method

Syntax Description

prompt-user	Specifies that no DID is set in the incoming POTS dial peer and that a Tcl script in the incoming POTS dial peer is used for two-stage dialing.
redialer	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device are used for two-stage dialing.

Command Default Prompt-user (when DID is not set in the dial peer)

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice access-method** command.

Usage Guidelines Use the **param access-method** command to specify the access method for two-stage dialing when DID is disabled in the POTS dial peer.

Examples The following example specifies prompt-user as the access method for two-stage dialing for the app_libretto_onramp9 IVR application:

```
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts
 param access-method prompt-user
```

Related Commands

Command	Description
call application voice access-method	Specifies the access method for two-stage dialing for the designated application.

param account-id-method

To configure an application to use a particular method to assign the account identifier, use the **param account-id-method** command in application parameter configuration mode. To remove configuration of this account identifier, use the **no** form of this command.

param account-id-method {**none** | **ani** | **dnis** | **gateway**}

no param account-id-method {**none** | **ani** | **dnis** | **gateway**}

Syntax Description

none	Account identifier is blank. This is the default.
ani	Account identifier is the calling party telephone number (automatic number identification, or ANI).
dnis	Account identifier is the dialed party telephone number (dialed number identification service, or DNIS).
gateway	Account identifier is a router-specific name derived from the hostname and domain name, displayed in the following format: router-name.domain-name.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice account-id-method** command.

Usage Guidelines

When an on-ramp application converts a fax into an e-mail, the e-mail contains a field called x-account-id, which can be used for accounting or authentication. The x-account-id field can contain information supplied as a result of this command, such as the calling party's telephone number (**ani**), the called party's telephone number (**dnis**), or the name of the gateway (**gateway**).

Examples

The following example sets the fax detection IVR application account identifier to the router-specific name derived from the hostname and domain name:

```
application
 service fax_detect flash:app_fax_detect.2.1.2.2.tcl
 param account-id-method gateway
```

Related Commands

Command	Description
call application voice account-id-method	Configures the fax detection IVR application to use a particular method to assign the account identifier.
param	Loads and configures parameters in a package or a service (application).
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param accounting enable

To enable authentication, authorization, and accounting (AAA) accounting for a Tool Command Language (TCL) application, use the **param accounting enable** command in application configuration mode. To disable accounting for a TCL application, use the **no** form of this command.

param accounting enable

no param accounting enable

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice accounting enable** command.

Usage Guidelines This command enables AAA accounting services if a AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions.

Examples The following example enables AAA accounting to be used with outbound store-and-forward fax:

```
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
 param accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

param accounting-list

To define the name of the accounting method list to be used for authentication, authorization, and accounting (AAA) with store-and-forward fax on a voice feature card (VFC), use the **param accounting-list** command in application configuration mode. To undefine the accounting method list, use the **no** form of this command.

param accounting-list *method-list-name*

no param accounting-list *method-list-name*

Syntax Description

method-list-name	Character string used to name a list of accounting methods to be used with store-and-forward fax.

Command Default No AAA accounting method list is defined

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice accounting-list** command.

Usage Guidelines This command defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists that are used in store-and-forward fax are applied globally.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store-and-forward fax functions on VFCs. The command is not used on modem cards.

Examples The following example defines a AAA accounting method list “smith” to be used with store-and-forward fax:

```
aaa new-model
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
 param accounting-list smith
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
param accounting enable	Enables AAA accounting for a TCL application.
mmoip aaa receive-accounting enable	Enables on-ramp AAA accounting services.

param authen-list

To specify the name of an authentication method list for a Tool Command Language (TCL) application, use the **param authen-list** command in global configuration mode. To disable the authentication method list for a TCL application, use the **no** form of this command.

param authen-list *method-list-name*

no param authen-list *method-list-name*

Syntax Description

method-list-name	Character string used to name a list of authentication methods to be used with T.38 fax relay and T.37 store-and-forward fax.

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice param authen-list** command.

Usage Guidelines This command defines the name of the authentication, authorization, and accounting (AAA) method list to be used with fax applications on voice feature cards. The method list itself, which defines the type of authentication services provided for store-and-forward fax, is defined using the **aaa authentication** command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), AAA method lists that are used with fax applications are applied globally.

After the authentication method lists have been defined, they are enabled by using the **param authentication enable** command.

Examples The following example defines a AAA authentication method list (called “fax”) to be used with T.38 fax relay and T.37 store-and-forward fax:

```
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
 param authen-list fax
 param authentication enable
```

Related Commands

Command	Description
aaa authentication	Enable AAA accounting of requested services for billing or security purposes.

Command	Description
param authen-method	Specifies the authentication method for a TCL application.
param authentication enable	Enables AAA authentication services for a TCL application.

param authen-method

To specify an authentication, authorization, and accounting (AAA) authentication method for a Tool Command Language (Tcl) application, use the **param authen-method** command in application configuration mode. To disable the authentication method for a Tcl application, use the **no** form of this command.

param authen-method {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

no param authen-method {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

prompt-user	User is prompted for the Tcl application account identifier.
ani	Calling party telephone number (automatic number identification or ANI) is used as the Tcl application account identifier.
dnis	Called party telephone number (dialed number identification service or DNIS) is used as the Tcl application account identifier.
gateway	Router-specific name derived from the host name and domain name is used as the Tcl application account identifier, displayed in the following format: *router-name.domain-name*.
redialer-id	Account string returned by the external redialer device is used as the Tcl application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer-dnis	Called party telephone number (dialed number identification service or DNIS) is used as the Tcl application account identifier captured by the redialer if a redialer device is present.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice authen-method** command in application configuration mode.

Usage Guidelines

Normally, when AAA is used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With T.37 store-and-forward fax and T.38 real-time fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication or that the user be prompted for the Tcl application.

Examples

The following example configures the router-specific name derived from the host name and domain name as the Tcl application account identifier for the app_libretto_onramp9 Tcl application:

```
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
 param authen-method gateway
```

Related Commands

Command	Description
param authentication enable	Enables AAA authentication services for a Tcl application.

param authentication enable

To enable authentication, authorization, and accounting (AAA) services for a Tool Command Language (TCL) application, use the **param authentication enable** command in application configuration mode. To disable authentication for a TCL application, use the **no** form of this command.

param authentication enable

no param authentication enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice authentication enable** command.

Usage Guidelines

This command enables AAA authentication services for a TCL application if a AAA authentication method list has been defined using the **aaa authentication** command and the **param authen-list** command.

Examples

The following example enables AAA authentication for an authentication method list (called "fax") with outbound store-and-forward fax.

```
application
 service app_libretto_onramp9 tftp://server-1/tftpboot/scripts/
 param authen-list fax
 param authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services when you use RADIUS or TACACS+.
param authen-list	Specifies the name of an authentication method list for a Tool Command Language (TCL) application.
param authen-method	Specifies the authentication method for a TCL application.

param convert-discpi-after-connect

To enable or disable conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state, use the **param convert-discpi-after-connect** command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param convert-discpi-after-connect {**enable** | **disable**}

no param convert-discpi-after-connect {**enable** | **disable**}

Syntax Description

enable	Convert a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
disable	Revert to a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Default

Enabled

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice default disc-prog-ind-at-connect** command.

Usage Guidelines

This command has no effect if the call is not in the active state. This command is available for the session_xwork package. If you are configuring this parameter for a package, you must first use the command **package session x_work**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace session_xwork convert-discpi-after-connect

Examples

The following example shows conversion enabled for a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8):

```
application
 package session_xwork
 param convert-discpi-after-connect enable
```

Related Commands

Command	Description
call application voice default disc-prog-ind-at-connect	Converts a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param dsn-script

To specify the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp delivery status notification (DSN) and message disposition notification (MDN) e-mail messages, use the **param dsn-script** command in application parameter configuration mode. To remove the application, use the **no** form of this command.

param dsn-script *application-name*

no param dsn-script *application-name*

Syntax Description

application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice dsn-script** command.

Usage Guidelines

When the off-ramp gateway receives a DSN or MDN e-mail message, it handles it in the same way as a voice e-mail trigger message. The dial peer is selected on the basis of dialed number identification service (DNIS), and the mail application hands off the call to the VoiceXML application that is configured with this command.

Examples

The following example shows how to define the DSN application and how to apply it to a dial peer:

```
application
 service offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
 param dsn-script dsn-mapp-test
!
dial-peer voice 1000 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
call application voice dsn-script	Specifies the VoiceXML application to which the off-ramp mail application hands off calls for off-ramp DSN and MDN e-mail messages.

param event-log

To enable or disable logging for linkable Tcl functions (packages), use the **param event-log** command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param event-log {**enable** | **disable**}

no param event-log {**enable** | **disable**}

Syntax Description

enable	Event logging is enabled.
disable	Event logging is disabled.

Command Default No default behavior or values

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice event-log** command.

Usage Guidelines This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace appcommon event-log

If you are configuring event logging for all voice applications, use the **event-log** command in application configuration monitor mode.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples The following example shows event-logging disabled for the built-in common voice application package:

```
application
 package appcommon
 param event-log disable
```

Related Commands

Command	Description
call application voice event-log	Enables event logging for a specific voice application.
event-log	Enables event logging for applications.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param fax-dtmf

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes, use the **param fax-dtmf** command in application parameter configuration mode. To remove configuration of this digit, use the **no** form of this command.

param fax-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

no param fax-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

Syntax Description

0 | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**	The telephone keypad digit processed by the calling party to indicate a fax call, in response to the audio prompt that plays during the default-voice or default-fax mode of the fax detection IVR application.

Command Default

2

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice fax-dtmf** command.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode as defined by the **param mode** command.

If you also configure voice DTMF using the **param voice-dtmf** command, you must use different numbers for the voice and fax DTMF digits.

Examples

The following example selects DTMF digit 1 to indicate a fax call:

```
application
 service faxdetect tftp://sample/tftp-users/tcl/app_fax_detect.2.x.x.tcl
 param fax-dtmf 1
```

Related Commands

Command	Description
call application voice fax-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes.
param mode	Configures the call transfer mode for a package.
param voice-dtmf	Directs an application to recognize a specified digit to indicate a voice call in default-voice and default-fax modes.

param global-password

To define a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card, use the **param global-password** command in application parameter configuration mode. To restore the default value, use the **no** form of this command.

param global-password *password*

no param global-password *password*

Syntax Description

password	Character string used to define the CiscoSecure for Windows NT password to be used with store-and-forward fax. The maximum length is 64 alphanumeric characters.

Command Default No password is defined

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice global-password** command.

Usage Guidelines CiscoSecure for Windows NT might require a separate password to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Windows NT server use this defined password.

This command applies to on-ramp store-and-forward fax functions on Cisco AS5300 universal access server voice feature cards. It is not used on modem cards.

Examples The following example shows a password (abercrombie) being used by AAA for the app_libretto_onramp9 Tcl application:

```
application
 service onramp tftp://sample/tftp-users/tcl/app_libretto_onramp9.tcl
 param global-password abercrombie
```

Related Commands

Command	Description
call application voice global-password	Defines a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card.

param language

To configure the language parameter in a service or package on the gateway, use the **param language** command in application parameter configuration mode. There is no **no** form of this command.

param language *prefix*

Syntax Description

prefix	Two-character prefix for the language; for example, "*en*" for English or "*ru*" for Russian.

Command Default No default behavior or values

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call language voice** command.

Usage Guidelines Before you configure the language parameter, you must load the language package using the **package language** command in application configuration mode.

If you are configuring this parameter for a service, use the following commands:

service *name url*

param language *prefix*

Examples The following example adds Russian (*ru*) as a Tcl module and configures the debitcard application to use Russian for prompts:

```
application
 package language ru tftp://box/unix/scripts/multi-lang/ru_translate.tcl
 service debitcard tftp://server-1/tftpboot/scripts/app_debitcard.2.0.2.8.tcl
  param language ru
```

Related Commands

Command	Description
call application voice set-location	Defines the category and location of audio files that are used for dynamic prompts by the specified IVR application (Tcl or VoiceXML).
call language voice	Configures an external Tcl module for use with an IVR application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.

Command	Description
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param mail-script

To specify the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers, use the **param mail-script** command in application parameter configuration mode. To remove the application, use the **no** form of this command.

param mail-script *application-name*

no param mail-script *application-name*

Syntax Description

application-name	Name of the VoiceXML application to which the off-ramp mail application hands off the call when the destination answers.

Command Default No default behavior or values

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice mail-script** command.

Usage Guidelines

- To configure the mail application onto the gateway, use the **application** command.
- The off-ramp mail application must be configured in the Multimedia Mail over Internet Protocol (MMoIP) dial peer that matches the telephone number contained in the header of the incoming e-mail message.
- The off-ramp mail application must use the Tool Command Language (Tcl) script named "app_voicemail_offramp.tcl" that is provided by Cisco. You can download this Tcl script from the Cisco website by following this path:

  Cisco.com > Technical Support & Documentation > Tools & Resources > Software Downloads > Access Software > TclWare

Examples The following example shows that the off-ramp mail application named "offramp-mapp" hands calls to the application named "mapp-test" if the telephone number in the e-mail header is seven digits beginning with 555:

```
application
service offramp-mapp tftp://sample/tftp-users/tcl/app_voicemail_offramp.tcl
param mail-script mapp-test
!
dial-peer voice 1001 mmoip
 application offramp-mapp
 incoming called-number 555....
 information-type voice
```

Related Commands

Command	Description
call application voice mail-script	Specifies the VoiceXML application to which the off-ramp mail application hands off a call when the destination telephone answers.

param mode

To configure the call transfer mode for a package, use the **param mode** command in application parameter configuration mode. To reset to the default, use the **no** form of this command.

param mode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}

no param mode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default Rotary method; call redirection is not invoked.

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines This command is used to configure call transfer mode for a package only. You can then configure one or more services to use that package. Alternatively, you can use the **paramspace callsetup mode** command to configure call transfer mode for a service, or standalone application.

Examples The following example shows the call transfer method set to redirect for the call setup package:

```
application
 package callsetup
 param mode redirect
```

Related Commands

Command	Description
call application voice mode	Directs the fax detection IVR application to operate in one of its four connection modes.
call application voice transfer mode	Specifies the call-transfer method for Tcl)or VoiceXML applications.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param pin-len

To define the number of characters in the personal identification number (PIN) for an application, use the **param pin-len** command in application parameter configuration mode. To disable the PIN for the designated application, use the **no** form of this command.

param pin-len *number*

no param pin-len *number*

Syntax Description

number	Number of allowable characters in PINs associated with the specified application. Range is from 0 to 10. The default is 4.

Command Default No default behavior or values

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice pin-len** command.

Usage Guidelines Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a PIN for the specified application and to pass that information to the specified application.

To configure the PIN length for a package, load the package using the **package** command before using the **param pin-len** command. To configure the PIN length for a service, use the **service** command before using the **param pin-len** command.

Examples The following example shows how to define a PIN length of 8 characters for a Tcl digit collection package:

```
application
 package digcl.tcl
 param pin-len 8
```

The following example shows how to define a PIN length of 8 characters for a debit card application:

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 param pin-len 8
```

Related Commands

Command	Description
call application voice pin-len	Defines the number of characters in the PIN for the designated application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param prompt

To direct the fax detection interactive voice response (IVR) application to use the specified audio file as a user prompt, use the **param prompt** command in application parameter configuration mode. To disable use of this audio file, use the **no** form of this command.

param prompt *prompt-url*

no param prompt *prompt-url*

Syntax Description

prompt-url	The URL or Cisco IOS file system (IFS) location on the TFTP server for the audio file containing the prompt for the application.

Command Default

The prompt space is empty and no prompt is played.

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice prompt** command.

Usage Guidelines

This command is useful only in the listen-first, default-voice, and default-fax modes of the fax detection application.

Audio files should be a minimum of 9 seconds long so that callers do not hear silence during the initial CNG detection period. Any .au file can be used; formats are described in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

Examples

The following example associates the audio file" promptfile.au" with the application file "fax_detect", and the application with the inbound POTS dial peer:

```
application
 service fax_detect tftp://users/scripts/app_fax_detect.2.x.x.tcl
 param mode default-voice
 param prompt promptfile.au
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice prompt	Directs the fax detection interactive voice response (IVR) application to use the specified audio file as a user prompt.

param redirect-number

To define the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application, use the **param redirect-number** command in application parameter configuration mode. To cancel the redirect telephone number, use the **no** form of this command.

param redirect-number *number*

no param redirect-number *number*

Syntax Description

number	Designated operator telephone number of the service provider (or any other number designated by the customer). This is the number where calls are terminated when, for example, allowed debit time has run out or the debit amount is exceeded.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice redirect-number** command.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the telephone number to which a call is redirected.

To configure the redirect number for a package, load the package using the **package** command before using the **param redirect-number** command. To configure the redirect number for a service, use the **service** command before using the **param redirect-number** command.

Examples

The following example shows how to define a redirect number for the application named “prepaid”:

```
application
 service prepaid tftp://tftp-server/scripts/prepaid.tcl
 param redirect-number 5550111
```

Related Commands

Command	Description
call application voice redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for the designated application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the personal identification number (PIN) for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
service	Loads and configures a specific, standalone application on a dial peer.

param reroutemode

To configure the call transfer reroutemode (call forwarding) for a package, use the **param reroutemode** command in application parameter configuration mode. To reset to the default, use the **no** form of this command.

param reroutemode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}

no param reroutemode

Syntax Description

redirect	Two call legs are directly connected. Supports RTPvt.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Two call legs are directly connected (redirect). If that fails, the two call legs are hairpinned on the gateway (rotary).
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two calls together. Release-to-Pivot (RTPvt) is not invoked. This is the default.

Command Default

Rotary method; RTPvt is not invoked.

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is used to configure call forwarding for a package only. You can then configure one or more services to use that package. Alternatively, you can use the **paramspace callsetup reroutemode** command to configure call forwarding for a service, or standalone application.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected, provided that the call leg is capable of it.

Examples

The following example shows the call forwarding method set to redirect for the call setup package:

```
application
 package callsetup
 param reroutemode redirect
```

Related Commands

Command	Description
call application voice transfer reroute-mode	Specifies the call-forwarding behavior of a Tcl application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param retry-count

To define the number of times that a caller is permitted to reenter the personal identification number (PIN) for a package, use the **param retry-count** command in application parameter configuration mode. To cancel the configured retry count, use the **no** form of this command.

param retry-count *number*

no param retry-count *number*

Syntax Description

number	Number of times the caller is permitted to reenter PIN digits. Range is 1 to 5. The default is 3.

Command Default 3

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define how many times a user can reenter a PIN.

To configure the PIN retry count for a package, load the package using the **package** command before using the **param retry-count** command. To configure the PIN retry count for a service, use the **service** command before using the **param retry-count** command.

Examples The following example shows how to configure the PIN retry count in a package so that a user can reenter a PIN two times before being disconnected.

```
application
 package sample1.tcl
 param retry-count 2
```

The following example shows how to configure the PIN retry count in a debit card application so that a user can reenter a PIN two times before being disconnected.

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 param retry-count 2
```

Related Commands

Command	Description
call application voice retry-count	Defines the number of times that a caller is permitted to reenter the PIN for the designated application.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param security

To configure security for linkable Tcl functions (packages), use the **param security** command in application parameter configuration mode. To restore this parameter to the default value, use the **no** form of this command.

param security {**trusted** | **untrusted**}

no param security {**trusted** | **untrusted**}

Syntax Description

trusted	Automatic number identification (ANI) is not blocked.
untrusted	ANI is blocked.

Command Default

No default behavior or values

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice security** command.

Usage Guidelines

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**.

If you are configuring this parameter for a service, use the following commands:

service *name url*

paramspace appcommon security {**trusted** | **untrusted**}

If an application is configured as a trusted application, it is trusted not to provide the calling number to the destination party, so ANI is always provided if available. Normally, the voice gateway does not provide the calling number (ANI) to a VoiceXML application if the caller ID is blocked. Caller ID is blocked if a call that comes into the voice gateway has the presentation indication field set to "presentation restricted". The session.telephone.ani variable is set to "blocked". When the **param security trusted** command is configured, the gateway does not block caller ID; it provides the calling number to the VoiceXML application. If the keyword of this command is set to untrusted, caller ID is blocked.

To enable GTD (Generic Transparency Descriptor) parameters in call signaling messages to map to VoiceXML and Tcl session variables, the **param security trusted** command must be configured. If this command is not configured, the VoiceXML variables that correspond to GTD parameters are marked as not available. For a detailed description of the VoiceXML and Tcl session variables, see the *Cisco VoiceXML Programmer's Guide* and the *Tcl IVR API Version 2.0 Programmer's Guide*, respectively.

Examples

The following example shows using the **param security trusted** command to set the security level of the common application package to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
 package appcommon
 param security trusted
```

Related Commands

Command	Description
call application voice security trusted	Sets the security level of a VoiceXML application to "trusted" so that ANI is not blocked.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
paramspace appcommon security	Configures security for a service (application).
param uid-length	Defines the number of characters in the UID for a package.
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
service	Loads and configures a specific, standalone application on a dial peer.

param uid-len

To define the number of characters in the user identification number (UID) for a package, use the **param uid-len** command in application parameter configuration mode. To restore the default setting for this command, use the **no** form of this command.

param uid-len *number*

no param uid-len *number*

Syntax Description

number	Number of allowable characters in UIDs that are associated with the specified application. Range is from 1 to 20. Default is 10.

Command Default

10 characters

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice uid-length** command.

Usage Guidelines

Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a UID.

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**. If you are configuring this parameter for a service, you must first use the **service** command

Examples

The following example configures the UID length to 20 in a package.

```
application
 package sample1.tcl
 param uid-len 20
```

The following example configures the UID length to 20 in a debit-card application.

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 param uid-len 20
```

Related Commands

Command	Description
call application voice uid-length	Defines the number of characters in the UID for the designated application and to pass that information to the specified application.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.

param voice-dtmf

To direct the fax detection interactive voice response (IVR) application to recognize a specified digit to indicate a voice call, use the **param voice-dtmf** command in application parameter configuration mode. To remove configuration of this digit, use the **no** form of this command.

param voice-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

no param voice-dtmf {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**}

Syntax Description

0 | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***** | **#**	The telephone keypad button pressed by the calling party to indicate a voice call, in response to the audio prompt configured in default-voice and default-fax mode of the fax detection IVR application.

Command Default

1

Command Modes

Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command is introduced to replace the **call application voice voice-dtmf** command.

Usage Guidelines

This command is useful only when the fax detection IVR application is being configured in default-voice mode or default-fax mode, as defined by the **param mode** command.

If you also configure voice DTMF using the **param voice-dtmf** command, you must use different numbers for the voice and fax DTMF digits.

Examples

The following example selects digit 2 Dual tone multifrequency (DTMF) to indicate a voice call:

```
application
 service faxdetect tftp://sample/tftp-users/tcl/app_fax_detect.2.x.x.tcl
 param voice-dtmf 2
dial-peer voice 302 pots
 application fax_detect
```

Related Commands

Command	Description
call application voice voice-dtmf	Directs the fax detection IVR application to recognize a specified digit to indicate a voice call.
param mode	Configures the call transfer mode for a package.
param fax-dtmf	Directs an application to recognize a specified digit to indicate a fax call in default-voice and default-fax modes.

param warning-time

To define the number of seconds of warning that a user receives before the allowed calling time expires use the **param warning-time** command in application parameter configuration mode. To remove the configured warning period, use the **no** form of this command.

param warning-time *number*

no param warning-time *number*

Syntax Description

number	Length of the warning period, in seconds, before the allowed calling time expires. Range is from 10 to 600. This argument has no default value.

Command Default No default behavior or values

Command Modes Application parameter configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice warning-time** command.

Usage Guidelines Use this command when configuring interactive voice response (IVR)—depending on the Tool Command Language (Tcl) script being used—or one of the IVR-related features (such as Debit Card) to define the number of seconds in the warning period before the allowed calling time expires.

This command is available for the built-in common voice application package. If you are configuring this parameter for that package, you must first use the command **package appcommon**. If you are configuring this parameter for a service, you must first use the **service** command

Examples The following example configures the warning time parameter to 30 seconds in a package.

```
application
 package sample1.tcl
 param warning-time 30
```

The following example configures the warning time parameter to 30 seconds in a debit-card application.

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 param warning-time 30
```

Related Commands

Command	Description
call application voice warning-time	Defines the number of seconds of warning that a user receives before the allowed calling time expires.
package appcommon	Configures parameters in the built-in common voice application package.
param	Loads and configures parameters in a package or a service (application).
param account-id-method	Configures an application to use a particular method to assign the account identifier.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with Progress Indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
param event-log	Enables or disables logging for linkable Tcl functions (packages).
param language	Configures the language parameter in a service or package on the gateway.
param mode	Configures the call transfer mode for a package.
param pin-len	Defines the number of characters in the PIN for an application.
param redirect-number	Defines the telephone number to which a call is redirected—for example, the operator telephone number of the service provider—for an application.
param reroutemode	Configures the call transfer reroutemode (call forwarding) for a package.
param retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
param security	Configures security for linkable Tcl functions (packages).
param uid-length	Defines the number of characters in theUID for a package.
service	Loads and configures a specific, standalone application on a dial peer.

paramspace

To enable an application to use parameters from the local parameter space of another application, use the **paramspace** command in application service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace *parameter-namespace parameter-name parameter-value*

no paramspace *parameter-namespace parameter-name parameter-value*

Syntax Description

parameter-namespace	Namespace of the parameter from which you want to use parameters.
parameter-name	Parameter to use.
parameter-value	Value of the parameter.

Command Default No default behavior or values

Command Modes Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines To avoid problems with applications using the same parameter names, the *parameter namespace,* or *parameterspace* concept is provided. When an application is defined on the gateway, its parameter namespace is automatically defined. This is known as the application's s local parameterspace. When you use the **param** command to configure an application's parameters, the parameters available for configuration are those contained in the local parameterspace.

If you want to use parameter definitions found in different parameterspace, you can use the **paramspace** *parameter-namespace parameter-name parameter-value* command to map the application's parameters to a different parameterspace. This allows that application to use the parameter definitions found in the new parameterspace, in addition to its local parameterspace.

Examples The following example shows a debit card service configured to use parameters from an English language translation package:

```
application
service debitcard tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
paramspace english language en
  paramspace english index 1
  paramspace english prefix en
  paramspace english location tftp://server-1//tftpboot/scripts/au/en/
```

Related Commands

Command	Description
param	Loads and configures parameters in a package or a service (application) on the gateway.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace appcommon event-log

To enable or disable logging for a service (application), use the **paramspace appcommon event-log** command in application service configuration mode. There is no **no** form of this command.

paramspace appcommon event-log {**enable** | **disable**}

Syntax Description

enable	Event logging is enabled.
disable	Event logging is disabled.

Command Default No default behavior or values

Command Modes Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice event-log** command.

Usage Guidelines Use this command to configure event logging for a service (application).

If you are configuring event logging for a package only, use the **package appcommon** command in application-parameter configuration mode.

If you are configuring event logging for all voice applications, use the **event-log** command in application-configuration monitor mode.

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples The following example shows event-logging disabled for a debit-card application.

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 paramspace appcommon event-log disable
```

Related Commands

Command	Description
call application voice event-log	Enables event logging for a specific voice application.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace appcommon security

To configure security for a service (application), use the **paramspace appcommon security** command in application service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace appcommon security {**trusted** | **untrusted**}

no paramspace appcommon security {**trusted** | **untrusted**}

Syntax Description

trusted	Automatic number identification (ANI) is not blocked.
untrusted	ANI is blocked.

Command Default

No default behavior or values

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice security** command.

Usage Guidelines

This command is available for the built-in common voice application package. If you are configuring this parameter for the built-in common voice application package, use the command **param security** command.

If an application is configured as a trusted application, it is trusted not to provide the calling number to the destination party, so ANI is always provided if available. Normally, the voice gateway does not provide the calling number (ANI) to a VoiceXML application if the caller ID is blocked. Caller ID is blocked if a call that comes into the voice gateway has the presentation indication field set to "presentation restricted". The session.telephone.ani variable is set to "blocked". When the **paramspace appcommon security trusted** command is configured, the gateway does not block caller ID; it provides the calling number to the VoiceXML application. If the keyword of this command is set to untrusted, caller ID is blocked.

To enable GTD (Generic Transparency Descriptor) parameters in call signaling messages to map to VoiceXML and Tcl session variables, the **paramspace appcommon security trusted** command must be configured. If this command is not configured, the VoiceXML variables that correspond to GTD parameters are marked as not available. For a detailed description of the VoiceXML and Tcl session variables, see the *Cisco VoiceXML Programmer's Guide* and the *Tcl IVR API Version 2.0 Programmer's Guide*, respectively.

Examples

The following example shows security configured for a debit card application. The security level of the application is set to "trusted" so that automatic number identification (ANI) is not blocked.

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 paramspace appcommon security trusted
```

Related Commands

Command	Description
call application voice security trusted	Sets the security level of a VoiceXML application to "trusted" so that ANI is not blocked.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace callsetup mode

To configure the call transfer mode for an application, use the **paramspace callsetup mode** command in application service configuration mode. To reset to the default, use the **no** form of this command.

paramspace callsetup mode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}

no paramspace callsetup mode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default

Rotary method; call redirection is not invoked.

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice transfer mode** command.

Usage Guidelines

Use this command to configure the call transfer mode for a service, or standalone application. Alternatively, you can use the **package callsetup** and **param mode** commands to configure call transfer mode for a package only, and then configure one or more services to use that package.

This command determines whether a voice application can invoke TBCT or RTPvt.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected if the call leg is capable of it.

Examples

The following example shows the call method set to redirect for a debit-card application:

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 paramspace callsetup mode redirect
```

Related Commands

Command	Description
call application voice transfer mode	Specifies the call-transfer method for Tcl)or VoiceXML applications.
package callsetup	Configures parameters in the built-in call-setup package.
param mode	Configures the call-transfer mode for a package.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace callsetup reroutemode

To configure the call reroute mode (call forwarding) for an application, use the **paramspace callsetup reroutemode** command in application service configuration mode. To reset to the default, use the **no** form of this command.

paramspace callsetup reroutemode {**redirect** | **redirect-at-alert** | **redirect-at-connect** | **redirect-rotary** | **rotary**}

no paramspace callsetup reroutemode

Syntax Description

redirect	Gateway redirects the call leg to the redirected destination number.
redirect-at-alert	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the alert state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports Two B-Channel Transfer (TBCT).
redirect-at-connect	Gateway places a new call to the redirected destination number and initiates a call transfer when the outgoing call leg is in the connect state. If the call transfer is successful, the two call legs are disconnected on the gateway. If the transfer fails, the gateway bridges the two call legs. Supports TBCT.
redirect-rotary	Gateway redirects the call leg to the redirected destination number. If redirection fails, the gateway places a rotary call to the redirected destination number and hairpins the two call legs. For TBCT, this mode is the same as **redirect-at-connect**.
rotary	Gateway places a rotary call for the outgoing call leg and hairpins the two call legs. Call redirection is not invoked. This is the default.

Command Default Rotary method; call redirection is not invoked.

Command Modes Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice transfer reroute-mode** command.

Usage Guidelines This command is used to configure the call forward mode for a service, or standalone application. Alternatively, you can use the **package callsetup param reroutemode** command to configure call forward mode for a package only, and then configure one or more services to use that package.

This command determines whether a voice application can invoke TBCT or RTPvt.

Redirect-rotary is the preferred transfer method because it ensures that a call-redirect method is always selected if the call leg is capable of it.

Examples

The following example shows the call forward method set to redirect for a debitcard application:

```
application
 service debitcard tftp://tftp-server/dc/app_debitcard.tcl
 paramspace callsetup reroutemode redirect
```

Related Commands

Command	Description
call application voice transfer reroute-mode	Specifies the call-forwarding behavior of a Tcl application.
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace language	Defines the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML).

paramspace language

To define the category and location of audio files that are used for dynamic prompts by an IVR application (Tcl or VoiceXML), use the **paramspace language** command in application service configuration mode. To remove these definitions, use the **no** form of this command.

To configure the language parameter in a service or package on the gateway, use the **param language** command in application service configuration mode.

paramspace *language* {**location** *location* | **index** *number* | **language** *prefix*}

Syntax Description

language	Name of the language package. Cisco IOS software includes some built-in language packages, such as English.
location *location*	URL of the audio files. Valid URLs refer to TFTP, FTP, HTTP, or RTSP servers, flash memory, or the removable disks on the Cisco 3600 series.
index *number*	Category group of the audio files (from 0 to 4). For example, audio files representing the days and months can be category 1, audio files representing units of currency can be category 2, and audio files representing units of time—seconds, minutes, and hours—can be category 3. Range is from 0 to 4; 0 means all categories.
language *prefix*	Two-character code that identifies the language associated with the audio files. Valid entries are as follows: • **en**—English • **sp**—Spanish • **ch**—Mandarin • **aa**—all

Command Default

No location, index, or category is set.

Command Modes

Application service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice language** and the **call application voice set-location** commands.

Usage Guidelines

Tcl scripts and VoiceXML documents can be stored in any of the following locations: On TFTP, FTP, or HTTP servers, in the flash memory on the gateway, or on the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations, and on RTSP servers.

You can configure multiple set-location lines for a single application.

With the Pre-Paid Debitcard Multi-Language feature, you can create Tcl scripts and a two-character code for any language. See the *Cisco Pre-Paid Debitcard Multi-Language Programmer's Reference*.

With the multilanguage support for Cisco IOS IVR, you can create a Tcl language module for any language and any set of Text-to-Speech (TTS) notations for use with Tcl and VoiceXML applications. See the *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response* document.

Examples

The following example shows how to configure the **paramspace language** command for a debitcard application.

```
application
service debitcard tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
paramspace english language en
  paramspace english index 1
  paramspace english prefix en
  paramspace english location tftp://server-1//tftpboot/scripts/au/en/
```

Related Commands

Command	Description
call application voice language	Specifies the language for dynamic prompts used by an IVR application (Tcl or VoiceXML).
call application voice set-location	Defines the category and location of audio files that are used for dynamic prompts by the specified IVR application (Tcl or VoiceXML).
paramspace	Enables an application to use parameters from the local parameter space of another application.
paramspace appcommon event-log	Enables or disables logging for a service (application).
paramspace appcommon security	Configures security for a service (application).
paramspace callsetup mode	Configures the call transfer mode for an application.
paramspace callsetup reroutemode	Configures the call reroute mode (call forwarding) for an application.

paramspace session_xwork convert-discpi-after-connect

To enable or disable conversion of a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state, use the **paramspace session_xwork convert-discpi-after-connect** command in application-service configuration mode. To return to the default parameter namespace for this parameter, use the **no** form of this command.

paramspace session_xwork convert-discpi-after-connect {**enable** | **disable**}

no paramspace session_xwork convert-discpi-after-connect {**enable** | **disable**}

Syntax Description

enable	Convert a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
disable	Revert to a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) when the call is in the active state.

Command Default

Enabled

Command Modes

Application-service configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application voice default disc-prog-ind-at-connect** command.

Usage Guidelines

This command has no effect if the call is not in the active state. If you are configuring this parameter for a package, use the **package session xwork** command.

Examples

The following example shows conversion enabled for a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8):

```
application
 service callappl.tcl tftp://tftp-server/callappl.tcl
 paramspace session_xwork convert-discpi-after-connect enable
```

Related Commands

Command	Description
call application voice default disc-prog-ind-at-connect	Converts a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
package session xwork	Configures parameters in the built-in session_xwork package.
param convert-discpi-after-connect	Enables or disables conversion of a DISCONNECT message with progress indicator set to PROG_INBAND (PI=8) to a regular DISCONNECT message when the call is in the active state.
paramspace	Enables an application to use parameters from the local parameter space of another application.

pattern

To match a call based on the entire Session Initiation Protocol (SIP) or telephone (TEL) uniform resource identifier (URI), use the **pattern** command in voice URI class configuration mode. To remove the match, use the **no** form of this command.

pattern *uri-pattern*

no pattern

Syntax Description

uri-pattern	Cisco IOS regular expression (regex) pattern that matches the entire URI. Can be up to 128 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- This command matches a regular expression pattern to the entire URI.
- When you use this command in a URI voice class, you cannot use any other pattern-matching command such as the **host**, **phone context**, **phone number**, or **user-id** commands.

Examples

The following example configures the voice class to match the entire SIP URI:

```
voice class uri r100 sip
 pattern elmo@cisco.com
```

Related Commands

Command	Description
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
phone number	Matches a call based on the phone number field in a TEL URI.

Command	Description
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

periodic-report interval

To configure periodic reporting parameters for gateway resource entities, use the **periodic-report interval** command in voice-class configuration mode. To disable the periodic reporting parameters configuration, use the **no** form of this command.

periodic-report interval *seconds*

no periodic-report interval *seconds*

Syntax Description

seconds	Periodic interval, in seconds. The range is from 30 to 21600.

Command Default The periodic interval report parameters are disabled.

Command Modes Voice-class configuration mode (config-class)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines Use the **periodic-report interval** command to periodically report the status of the monitoring resources to the external entity. The triggering takes place based on the preconfigured interval value. You can use the statistics collected by this method of reporting to collect information on resource usage.

Examples The following example shows how to configure a resource group to trigger reporting every 180 seconds:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 1
Router(config-class)# periodic-report interval 180
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

permit hostname (SIP)

To store hostnames used during validatation of initial incoming INVITE messages, use the **permit hostname** command in SIP-ua configuration mode. To remove a stored hostname, use the **no** form of this command.

permit hostname dns: *domain name*

no permit hostname

Syntax Description

dns: *domain name*	Domain name in DNS format. Domain names can be up to 30 characters in length; domain names exceeding 30 characters will be truncated.

Command Modes

SIP-ua configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **permit hostname** command allows you to specify hostnames in FQDN (fully qualified domain name) format used during validation of incoming initial INVITE messages. The length of the hostname can be up to 30 characters; hostnames exceeding 30 characters will be truncated. You can store up to 10 hostnames by repeating the **permit hostname** command.

Once configured, initial INVITEs with a hostname in the requested Universal Resource Identifier (URI) are compared to the configured list of hostnames. If there is a match, the INVITE is processed; if there is a mismatch, a “400 Bad Request - Invalid Host” is sent, and the call is rejected.

Note Before Software Release 12.4(9)T, hostnames in incoming INVITE-request messages were only validated when they were in IPv4 format; now you can specify hostnames in fully qualified domain name (FQDN) format.

Examples

The following example show you how to set the hostname to sip.example.com:

```
Router(config)# sip-ua
Router(conf-sip-ua)# permit hostname dns:sip.example.com
```

phone context

To filter out uniform resource identifiers (URIs) that do not contain a phone-context field that matches the configured pattern, use the **phone context** command in voice URI class configuration mode. To remove the pattern, use the **no** form of this command.

phone context *phone-context-pattern*

no phone context

Syntax Description

phone-context-pattern	Cisco IOS regular expression pattern to match against the phone context field in a SIP or TEL URI. Can be up to 32 characters.

Command Default No default behavior or values

Command Modes Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command with at least one other pattern-matching command, such as **host**, **phone number**, or **user-id**; using it alone does not result in any matches on the voice class.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples The following example sets a match on the phone context in the URI voice class:

```
voice class uri 10 tel
 phone number ^408
 phone context 555
```

Related Commands

Command	Description
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone number	Matches a call based on the phone number field in a TEL URI.

Command	Description
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

phone number

To match a call based on the phone-number field in a telephone (TEL) uniform resource identifier (URI), use the **phone number** command in voice URI class configuration mode. To remove the pattern, use the **no** form of this command.

phone number *phone-number-pattern*

no phone number

Syntax Description

phone-number-pattern	Cisco IOS regular expression pattern to match against the phone-number field in a TEL URI. Can be up to 32 characters.

Command Default No default behavior or values

Command Modes Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command only in a voice class for TEL URIs.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples The following example defines a voice class that matches on the phone number field in a TEL URI:

```
voice class uri r101 tel
 phone number ^408
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class to use for matching the destination URI that is supplied by a voice application.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

pickup direct

To define a feature code for a Feature Access Code (FAC) to access Pickup Direct on an analog phone, use the **pickup direct** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup direct *keypad-character*

no pickup direct

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 6. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default The default value is 6.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Pickup Direct from the default (6) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a feature access code (FAC) consisting of a prefix plus a feature code, for example **6. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another FAC, a speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Note This FAC is not supported by Cisco Unified Communications Manager.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (6). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##3 on the keypad and then the ringing extension number to pick up an incoming call.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup direct 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup group	Defines a feature code for a feature access code (FAC) to Group Call Pickup from another group.
pickup local	Defines a feature code for a feature access code (FAC) to Group Call Pickup from the local group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).

Command	Description
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) in STC application and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

pickup group

To define a feature code for a feature access code (FAC) to access Group Call Pickup on an analog phone, use the **pickup group** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup group *keypad-character*

no pickup group

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 4. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.4(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#)

Command Default The default value is 4.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines This command changes the value of the feature code for Pickup Direct from the default (4) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **4. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another feature code, a speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (4). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. After these values are configured, a phone user must press ##3 on the keypad, then the pickup-group number for the ringing extension number to pick up the incoming call.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup direct 3
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup direct	Defines a feature code for a feature access code (FAC) for Direct Call Pickup of a ringing extension number.
pickup local	Defines a feature code for a feature access code (FAC) for Group Call Pickup to pick up an incoming call from the local group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

pickup local

To define a a feature code for a Feature Access Code (FAC) to access Group Call Pickup for a local group on an analog phone, use the **pickup local** command in STC application feature access-code configuration mode. To return the code to its default, use the **no** form of this command.

pickup local *keypad-character*

no pickup local

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad. Default: 3. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.5(20)YA and later releases, the string can be any o the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default The default value is 3.

Command Modes STC application feature access-code configuration (config-stcapp-fac)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the feature code for Local Group Pickup from the default (3) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **3. If the feature code is 78#, the phone user dials only 78#, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already configured for another feature code or speed-dial code, or for the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by another feature code or speed-dial code, or by the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the feature code for Pickup Direct from the default (3). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##9 on the keypad to pick up an incoming call in the same group as this extension number.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# pickup local 9
Router(config-stcapp-fac)# exit
```

Related Commands

Command	Description
pickup direct	Defines a feature code for a feature access code (FAC) for Direct Call Pickup of a ringing extension number.
pickup group	Defines a feature code for a feature access code (FAC) for Group Call Pickup to pick up an incoming call from another group.
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).
stcapp feature access-code	Enables feature access codes (FACs) in STC application and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

playout-delay (dial peer)

To tune the playout buffer on digital signal processors (DSPs) to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in dial peer configuration mode. To reset the playout buffer to the default, use the **no** form of this command.

playout-delay {**fax** *milliseconds* | **maximum** *milliseconds* | **minimum** {**default** | **low** | **high**} | **nominal** *milliseconds*}

no playout-delay {**fax** | **maximum** | **minimum** | **nominal**}

Syntax Description

fax *milliseconds*	Amount of playout delay that the jitter buffer should apply to fax calls, in milliseconds. Range is from 0 to 700. Default is 300.
maximum *milliseconds*	(Adaptive mode only) Upper limit of the jitter buffer, or the highest value to which the adaptive delay is set, in milliseconds. Range is from 40 to 1700, although this value depends on the type of DSP and how the voice card is configured for codec complexity. (See the **codec complexity** command.) Default is 200. If the voice card is configured for high codec complexity, the highest value that can be configured for **maximum** for compressed codecs is 250 ms. For medium-complexity codec configurations, the highest **maximum** value is 150 ms. Voice hardware that does not support the voice card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 200 ms.
minimum	(Adaptive mode only) Lower limit of the jitter buffer, or the lowest value to which the adaptive delay is set, in milliseconds. Values are as follows: • **default—**40 ms. Use when there are normal jitter conditions in the network. This is the default. • **low—**10 ms. Use when there are low jitter conditions in the network. • **high—**40 ms. Use when there are high jitter conditions in the network.
nominal *milliseconds*	Amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway, in milliseconds. In fixed mode, this is also the maximum size of the jitter buffer throughout the call. Range is from 0 to 1500, although this value depends on the type of DSP and how the voice card is configured for codec complexity. Default is 60. For non-conference calls when you are using DSPware version 4.1.33 or a later version, the following values are allowed. • If the voice card is configured for high codec complexity, the highest value that can be configured for the **nominal** keyword for compressed codecs is 200 ms. • For medium-complexity codec configurations, the highest nominal value is 150 ms.

nominal *milliseconds* (continued)

For conference calls when you are using DSPware version 4.1.33 or a later version, the following values are allowed:

- The first decoder stream can be assigned a nominal value as high as 200 ms (high-complexity codec) or 150 ms (medium-complexity codec).
- Subsequent decoder streams are limited to the highest nominal value of 150 ms (high-complexity) or 80 ms (medium-complexity).

When the playout-delay mode is configured for fixed operation and setting the expected jitter buffer size with the nominal value, the minimum effective value for the playout delay will depend on the codec in use and the configured minimum value.

- When the **playout-delay minimum low** is configured the minimum actual jitter buffer size will be 30ms even when setting the nominal to a value lower than 30msec.
- When the **playout-delay minimum default**, the minimum jitter buffer size when running in fixed mode will be 60ms.

When fixed mode is configured, there is a 10msec added to the nominal value when setting the jitter buffer when configured for G.729 and a 5ms added using G.711

Voice hardware that does not support the voice-card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 200 ms for the first decoder stream and 150 ms for subsequent decoder streams.

Note With DSPware versions earlier than 4.1.33, the highest nominal value that can be configured is 150 ms for high-complexity codec configurations and analog modules. The highest nominal value for medium-complexity codec configurations is 80 ms.

Defaults

fax—300 milliseconds
maximum—200 milliseconds
minimum—default (40 milliseconds)
nominal—60 milliseconds

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	This command was implemented on the Cisco ICS7750.

Release	Modification
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for dial peer configuration mode was added on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco MC3810, Cisco AS5200, Cisco AS5300, Cisco AS5400, and Cisco AS5800. The **minimum** keyword was introduced.
12.2(13)T	The **fax** keyword was introduced.
12.2(13)T8	DSPware version 4.1.33 was implemented.

Usage Guidelines

Before Cisco IOS Release 12.1(5)T, this command was used in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the Voice over IP (VoIP) dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout-delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

Playout delay is the amount of time that elapses between the time at which a voice packet is received at the jitter buffer on the DSP and the time at which it is played out to the codec. In most networks with normal jitter conditions, the defaults are adequate and you will not need to configure this command.

In situations in which you want to improve voice quality by reducing jitter or you want to reduce network delay, you can configure playout-delay parameters. The parameters are slightly different for each of the two playout-delay modes, adaptive and fixed (see the **playout-delay mode** command).

In adaptive mode, the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured. The maximum limit establishes the highest value to which the adaptive delay is set. The minimum limit is the low-end threshold for the delay of incoming packets by the adaptive jitter buffer. Algorithms in the DSPs that control the growth and shrinkage of the jitter buffer are weighted toward the improvement of voice quality at the expense of network delay: jitter buffer size increases rapidly in response to spikes in network transmissions and decreases slowly in response to reduced congestion.

In fixed mode, the nominal value is the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway and is also the maximum size of the jitter buffer throughout the call.

As a general rule, if there is excessive breakup of voice due to jitter with the default playout-delay settings, increase playout delay times. If your network is small and jitter is minimal, decrease playout-delay times for a smaller overall delay.

When there is bursty jitter in the network, voice quality can be degraded even though the jitter buffer is actually adjusting the playout delay correctly. The constant readjustment of playout delay to erratic network conditions causes voice quality problems that are usually alleviated by increasing the minimum playout delay-value in adaptive mode or by increasing the nominal delay for fixed mode.

Use the **show call active voice** command to display the current delay, as well as high- and low-water marks for delay during a call. Other fields that can help determine the size of a jitter problem are ReceiveDelay, GapFillWith..., LostPackets, EarlyPackets, and LatePackets. The following is sample output from the **show call active voice** command:

```
VOIP:
     ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
     IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
     RemoteIPAddress=192.168.100.101
     RemoteUDPPort=18834
     RoundTripDelay=26 ms
     SelectedQoS=best-effort
     tx_DtmfRelay=inband-voice
     FastConnect=TRUE
     Separate H245 Connection=FALSE
     H245 Tunneling=FALSE
     SessionProtocol=cisco
     SessionTarget=
     OnTimeRvPlayout=417000
     GapFillWithSilence=850 ms
     GapFillWithPrediction=2590 ms
     GapFillWithInterpolation=0 ms
     GapFillWithRedundancy=0 ms
     HiWaterPlayoutDelay=70 ms
     LoWaterPlayoutDelay=29 ms
     ReceiveDelay=39 ms
     LostPackets=0
     EarlyPackets=0
     LatePackets=86
```

Examples

The following example uses default adaptive mode with a minimum playout delay of 10 ms and a maximum playout delay of 60 ms on VoIP dial peer 80. The size of the jitter buffer is adjusted up and down on the basis of the amount of jitter that the DSP finds, but is never smaller than 10 ms and never larger than 60 ms.

```
dial-peer 80 voip
 playout-delay minimum low
 playout-delay maximum 60
```

Related Commands

Command	Description
codec complexity	Specifies call density and codec complexity based on the codec standard you are using.
playout-delay (voice-port)	Tunes the playout buffer to accommodate packet jitter caused by switches in the WAN.
playout-delay mode	Selects fixed or adaptive mode for the jitter buffer on DSPs.
show call active voice	Displays active call information for voice calls.

playout-delay (voice-port)

To tune the playout buffer to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in voice-port configuration mode. To reset the playout buffer to the default, use the **no** form of this command.

playout-delay {**fax** | **maximum** | **nominal**} *milliseconds*

no playout-delay {**fax** | **maximum** | **nominal**}

Syntax Description

fax *milliseconds*	Amount of playout delay that the jitter buffer should apply to fax calls, in milliseconds. Range is from 0 to 700. Default is 300.
maximum *milliseconds*	Delay time that the digital signal processor (DSP) allows before starting to discard voice packets, in milliseconds. Range is from 40 to 320. Default is 160.
nominal *milliseconds*	Initial (and minimum allowed) delay time that the DSP inserts before playing out voice packets, in milliseconds. Range is from 40 to 200. Default is 80.

Defaults

fax—300 milliseconds
maximum—160 milliseconds
nominal—80 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(13)T	The **fax** keyword was added.

Usage Guidelines

If there is excessive breakup of voice due to jitter with the default playout delay settings, increase the delay times. If your network is small and jitter is minimal, decrease the delay times to reduce delay.

Before Cisco IOS Release 12.1(5)T, th**e playout-delay c**ommand was configured in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the Voice over IP (VoIP) dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout-delay values have been configured on a voice port and on a dial peer, the dial-peer configuration takes precedence.

Playout delay is the amount of time that elapses between the time at which a voice packet is received at the jitter buffer on the DSP and the time at which it is played out to the codec. In most networks with normal jitter conditions, the defaults are adequate and you will not need to configure the **playout-delay** command.

In situations in which you want to improve voice quality by reducing jitter or you want to reduce network delay, you can configure playout-delay parameters. The parameters are slightly different for each of the two playout-delay modes, adaptive and fixed (see the **playout-delay mode** command).

In adaptive mode, the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured. The maximum limit establishes the highest value to which the adaptive delay will be set. The minimum limit is the low-end threshold for incoming packet delay that is created by the adaptive jitter buffer. Algorithms in the DSPs that control the growth and shrinkage of the jitter buffer are weighted toward the improvement of voice quality at the expense of network delay: jitter buffer size increases rapidly in response to spikes in network transmissions and decreases slowly in response to reduced congestion.

In fixed mode, the nominal value is the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway and is also the maximum size of the jitter buffer throughout the call.

As a general rule, if there is excessive breakup of voice due to jitter with the default playout-delay settings, increase playout-delay times. If your network is small and jitter is minimal, decrease playout-delay times for a smaller overall delay.

When there is bursty jitter in the network, voice quality can be degraded even though the jitter buffer is actually adjusting the playout delay correctly. The constant readjustment of playout delay to erratic network conditions causes voice quality problems that are usually alleviated by increasing the minimum playout-delay value in adaptive mode or by increasing the nominal delay for fixed mode.

Note The minimum limit for playout delay is configured using the **playout-delay** (dial peer) command.

Use the **show call active voice** command to display the current delay, as well as high- and low-water marks for delay during a call. Other fields that can help determine the size of a jitter problem are GapFillWith..., ReceiveDelay, LostPackets, EarlyPackets, and LatePackets. The following is sample output from the **show call active voice** command:

```
VOIP:
     ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
     IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
     RemoteIPAddress=192.168.100.101
     RemoteUDPPort=18834
     RoundTripDelay=26 ms
     SelectedQoS=best-effort
     tx_DtmfRelay=inband-voice
     FastConnect=TRUE
     Separate H245 Connection=FALSE
     H245 Tunneling=FALSE
     SessionProtocol=cisco
     SessionTarget=
     OnTimeRvPlayout=417000
     GapFillWithSilence=850 ms
     GapFillWithPrediction=2590 ms
     GapFillWithInterpolation=0 ms
     GapFillWithRedundancy=0 ms
     HiWaterPlayoutDelay=70 ms
     LoWaterPlayoutDelay=29 ms
     ReceiveDelay=39 ms
```

```
LostPackets=0
EarlyPackets=0
LatePackets=86
```

Examples

The following example sets nominal playout delay to 80 ms and maximum playout delay to 160 ms on voice port 1/0/0:

```
voice-port 1/0/0
 playout-delay nominal 80
 playout-delay maximum 160
```

Related Commands

Command	Description
playout-delay (dial peer)	Tunes the playout buffer on DSPs to accommodate packet jitter caused by switches in the WAN.
playout-delay mode	Selects fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors.
show call active	Shows active call information for voice calls or fax transmissions in progress.
vad	Enables voice activity detection.

playout-delay mode (dial peer)

To select fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors (DSPs), use the **playout-delay mode** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

playout-delay mode {**adaptive** | **fixed**}

no playout-delay mode

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Command Default Adaptive jitter buffer size

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco MC3810, and Cisco ICS 7750. The **no-timestamps** keyword was removed.

Usage Guidelines Before Cisco IOS Release 12.1(5)T, this command was used only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial peer configuration mode.

Tip When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial peer configuration takes precedence.

In most networks with normal jitter conditions, the default is adequate and you do not need to configure this command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example sets adaptive playout-delay mode with a high (80 ms) minimum delay on a VoIP dial peer 80:

```
dial-peer 80 voip
 playout-delay mode adaptive
 playout-delay minimum high
```

Related Commands

Command	Description
playout-delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

playout-delay mode (voice-port)

To select fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors (DSPs), use the **playout-delay mode** command in voice port configuration mode. To reset to the default, use the **no** form of this command.

playout-delay mode {**adaptive** | **fixed**}

no playout-delay mode

Syntax Description

adaptive	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
fixed	Jitter buffer size does not adjust during a call; a constant playout delay is added.

Command Default Adaptive jitter buffer size

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)XI	This command was implemented on the Cisco ICS 7750. The keyword **mode** was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and the **no-timestamps** keyword was removed.

Usage Guidelines Before Cisco IOS Release 12.1(5)T, this command was used only in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be used in dial peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial peer configuration mode.

Tip When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If conflicting playout delay values have been configured on a voice port and on a dial peer, the dial peer configuration takes precedence.

In most networks with normal jitter conditions, the default is adequate and you do not need to configure the **playout-delay mode** command.

The default is adaptive mode, in which the average delay for voice packets varies depending on the amount of interarrival variation that packets have as the call progresses. The jitter buffer grows and shrinks to compensate for jitter and to keep voice packets playing out smoothly, within the maximum and minimum limits that have been configured.

Select fixed mode only when you understand your network conditions well, and when you have a network with very poor quality of service (QoS) or when you are interworking with a media server or similar transmission source that tends to create a lot of jitter at the transmission source. In most situations it is better to configure adaptive mode and let the DSP size the jitter buffer according to current conditions.

Examples

The following example sets fixed mode on a Cisco 3640 voice port with a nominal delay of 80 ms.

```
voice-port 1/1/0
 playout-delay mode fixed
 playout-delay nominal 80
```

Related Commands

Command	Description
playout-delay	Tunes the jitter buffer on DSPs for playout delay of voice packets.
show call active voice	Displays active call information for voice calls.

port (Annex G neighbor BE)

To configure the port number of the neighbor that is used for exchanging Annex G messages, use the **port** command in Annex G Neighbor BE configuration mode. To remove the port number, use the **no** form of this command.

port *neighbor-port*

no port

Syntax Description

neighbor-port	Port number of the neighbor. This number is used for exchanging Annex G messages. The default port number is 2099.

Defaults

2099

Command Modes

Annex G Neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

When cofiguring the **no port** command the *neighbor-port* argument is not used.

Examples

The following example sets a neighbor BE to port number 2010.

```
Router(config-annexg-neigh)# port 2010
```

Related Commands

Command	Description
advertise (annex g)	Controls the types of descriptors that the BE advertises to its neighbors.
cache	Configures the local BE to cache the descriptors received from its neighbors.
id	Configures the local ID of the neighboring BE.
query-interval	Configures the interval at which the local BE will query the neighboring BE.

port (dial-peer)

To associate a dial peer with a specific voice port, use the **port** command in dial peer configuration mode. To cancel this association, use the **no** form of this command.

Cisco 1750 and Cisco 3700 Series

port *slot-number*/*port*

no port *slot-number*/*port*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

no port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-number*}

Cisco AS5300 and Cisco AS5800

port *controller-number*:**D**

no port *controller-number*:**D**

Cisco uBR92x Series

port *slot*/*subunit*/*port*

no port *slot*/*subunit*/*port*

Syntax Description

Cisco 1750 and Cisco 3700 Series

slot-number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which the VIC has been installed.
port	Voice port number. Valid entries are 0 and 1.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 and 1.
port	Voice port number. Valid entries are 0 and 1.
slot	Router location in which the voice port adapter is installed. Valid entries are 0 and 3.
port	Voice interface card location. Valid entries are 0 and 3.
ds0-group-number	The DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300

controller-number	The T1 or E1 controller.
:D	Indicates the D channel associated with the ISDN PRI.

Cisco uBR92x series

slot/*subunit*/*port*	The analog voice port. Valid entries for the *slot*/*subunit*/*port* are as follows: • *slot*—A router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit*—A VIC in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port*—An analog voice port number. Valid entries are 0 and 1.

Command Default

No port is configured.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(3)T	This command was implemented on the Cisco 2600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco uBR924.
12.0(7)T	This command was implemented on the Cisco AS5800.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

This command enables calls that come from a telephony interface to select an incoming dial peer and for calls that come from the VoIP network to match a port with the selected outgoing dial peer.

This command applies only to POTS peers.

Note This command does not support the extended EC feature on the Cisco AS5300.

Examples

The following example associates POTS dial peer 10 with voice port 1, which is located on subunit 0 and accessed through port 0:

```
dial-peer voice 10 pots
 port 1/0/0
```

The following example associates POTS dial peer 10 with voice port 0:D:

```
dial-peer voice 10 pots
 port 0:D
```

The following example associates POTS dial peer 10 with voice port 1/0/0:D (T1 card):

```
dial-peer voice 10 pots
 port 1/0/0:D
```

Related Commands

Command	Description
prefix	Specifies the prefix of the dialed digits for a dial peer.

port (MGCP profile)

To associate a voice port with the Media Gateway Control Protocol (MGCP) profile that is being configured, use the **port** command in MGCP profile configuration mode. To disassociate the voice port from the profile, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Voice port or DS0-group number to be used as an MGCP endpoint associated with an MGCP profile.

Command Default

No default behavior or values

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced as the **voice-port** (MGCP profile) command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was renamed the **port** (MGCP profile) command.

Usage Guidelines

This command is used when values for an MGCP profile are configured.

This command associates a voice port with the MGCP profile that is being defined. To associate multiple voice ports with a profile, repeat this command with different voice port arguments.

This command is not used when the default MGCP profile is configured because the values in the default profile configuration apply to all parameters that have not been otherwise configured for a user-defined MGCP profile.

Examples

The following example associates an analog voice port with an MGCP profile on a Cisco uBR925 platform:

```
Router(config)# mgcp profile ny110ca
Router(config-mgcp-profile)# port 0
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

port (supplementary-service)

To enter the supplementary-service voice-port configuration mode for associating a voice port with STC application supplementary-service features, use the **port** command in supplementary-service configuration mode. To cancel the association, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	Location of port in Cisco ISR or Cisco VG224 Analog Phone Gateway. Syntax is platform-dependent; type **?** to determine.

Command Default This command has no default behavior or values.

Command Modes Supplementary-service configuration (config-stcapp-suppl-serv)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines This command associates an analog FXS port to STC application supplementary-service features being configured.

Examples The following example shows how to enable Hold/Resume on analog endpoints connected to port 2/0 of a Cisco VG224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
hold-resume	Enables Hold/Resume in Feature mode on the port being configured.

port media

To specify the serial interface to which the local video codec is connected for a local video dial peer, use the **port media** command in video dial peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

port media *interface*

no port media

Syntax Description

interface	Serial interface to which the local codec is connected. Valid entries are 0 and 1.

Command Default No interface is specified

Command Modes Video dial peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example specifies serial interface 0 as the specified interface for the codec local video dial peer 10:

```
dial-peer video 10 videocodec
 port media Serial0
```

Related Commands

Command	Description
port signal	Specifies the slot location of the VDM and the port location of the EIA/TIA-366 interface for signaling.
show dial-peer video	Displays dial peer configuration.

port signal

To specify the slot location of the video dialing module (VDM) and the port location of the EIA/TIA-366 interface for signaling for a local video dial peer, use the **port signal** command in video dial peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

port signal *slot*/*port*

no port signal

Syntax Description

slot	Slot location of the VDM. Valid values are 1 and 2.
port	Port location of the EIA/TIA-366 interface.

Command Default No locations are specified

Command Modes Video dial peer configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM video dial peer configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example sets up the VDM and EIA/TIA-366 interface locations for the local video dial peer designated as 10:

```
dial-peer video 10 videocodec
 port signal 1/0
```

Related Commands

Command	Description
port media	Specifies the serial interface to which the local video codec is connected.
show dial-peer video	Displays dial peer configuration.

pots call-waiting

To enable the local call-waiting feature, use the global configuration **pots call-waiting** command in global configuration mode. To disable the local call-waiting feature, use the **no** form of this command.

pots call-waiting {**local** | **remote**}

no pots call-waiting {**local** | **remote**}

Syntax Description

local	Enable call waiting on a local basis for the routers.
remote	Rely on the network provider service instead of the router to hold calls.

Command Default

Remote, in which case the call- holding pattern follows the settings of the service provider rather than those of the router.

Command Modes

Global configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Usage Guidelines

To display the call-waiting setting, use the **show running-config** or **show pots status** command. The ISDN call waiting service is used if it is available on the ISDN line connected to the router even if local call waiting is configured on the router. That is, if the ISDN line supports call waiting, the local call waiting configuration on the router is ignored.

Examples

The following example enables local call waiting on a router:

```
pots call-waiting local
```

Related Commands

Command	Description
call-waiting	Configures call waiting for a specific dial peer.
show pots status	Displays the settings of the physical characteristics and other information on the telephone interfaces of a Cisco 800 series router.

pots country

To configure your connected telephones, fax machines, or modems to use country-specific default settings for each physical characteristic, use the **pots country** command in global configuration mode. To disable the use of country-specific default settings, use the **no** form of this command.

pots country *country*

no pots country *country*

Syntax Description

country	Country in which your router is located.

Command Default

A default country is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to the Cisco 800 series routers.

If you need to change a country-specific default setting of a physical characteristic, you can use the associated command listed in the "Related Commands" section. Enter the **pots country ?** command to get a list of supported countries and the code you must enter to indicate a particular country.

Examples

The following example specifies that the devices connected to the telephone ports use default settings specific to Germany for the physical characteristics:

```
pots country de
```

Related Commands

Command	Description
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots dialing-method

To specify how the router collects and sends digits dialed on your connected telephones, fax machines, or modems, use the **pots dialing-method** command in global configuration mode. To disable the specified dialing method, use the **no** form of this command.

pots dialing-method {**overlap** | **enblock**}

no pots dialing-method {**overlap** | **enblock**}

Syntax Description

overlap	The router sends each digit dialed in a separate message.
enblock	The router collects all digits dialed and sends the digits in one message.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

To interrupt the collection and transmission of dialed digits, enter a pound sign (#), or stop dialing digits until the interdigit timer runs out (10 seconds).

Examples

The following example specifies that the router uses the enblock dialing method:

```
pots dialing-method enblock
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots disconnect-supervision

To specify how a router notifies the connected telephones, fax machines, or modems when the calling party has disconnected, use the **pots disconnect-supervision** command in global configuration mode. To disable the specified disconnect method, use the **no** form of this command.

pots disconnect-supervision {**osi** | **reversal**}

no pots disconnect-supervision {**osi** | **reversal**}

Syntax Description

osi	Open switching interval (OSI) is the duration for which DC voltage applied between tip and ring conductors of a telephone port is removed.
reversal	Polarity reversal of tip and ring conductors of a telephone port.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Most countries except Japan typically use the **osi** option. Japan typically uses the **reversal** option.

Examples

The following example specifies that the router uses the OSI disconnect method:

```
pots disconnect-supervision osi
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots disconnect-time

To specify the interval in which the disconnect method is applied if your connected telephones, fax machines, or modems fail to detect that a calling party has disconnected, use the **pots disconnect-time** command in global configuration mode. To disable the specified disconnect interval, use the **no** form of this command.

pots disconnect-time *interval*

no pots disconnect-time interval

Syntax Description

interval	Interval, in milliseconds. Range is from 50 to 2000.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

The **pots disconnect-supervision** command configures the disconnect method.

Examples

The following example specifies that the connected devices apply the configured disconnect method for 100 ms after a calling party disconnects:

```
pots disconnect-time 100
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots distinctive-ring-guard-time

To specify the delay in which a telephone port can be rung after a previous call is disconnected, use the **pots distinctive-ring-guard-time** command in global configuration mode. To disable the specified delay, use the **no** form of this command.

pots distinctive-ring-guard-time *milliseconds*

no pots distinctive-ring-guard-time *milliseconds*

Syntax Description

milliseconds	Delay, in milliseconds. Range is from 0 to 1000.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example specifies that a telephone port can be rung 100 ms after a previous call is disconnected:

```
pots distinctive-ring-guard-time 100
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots encoding

To specify the pulse code modulation (PCM) encoding scheme for your connected telephones, fax machines, or modems, use the **pots encoding** command in global configuration mode. To disable the specified scheme, use the **no** form of this command.

pots encoding {**alaw** | **ulaw**}

no pots encoding {**alaw** | **ulaw**}

Syntax Description

alaw	A-law. International Telecommunication Union Telecommunication Standardization Section (ITU-T) PCM encoding scheme used to represent analog voice samples as digital values.
ulaw	Mu-law. North American PCM encoding scheme used to represent analog voice samples as digital values.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Europe typically uses a-law. North America typically uses u-law.

Examples

The following example specifies a-law as the PCM encoding scheme:

```
pots encoding alaw
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.

Command	Description
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots forwarding-method

To configure the type of call-forwarding method to be used for Euro-ISDN (formerly NET3) switches, use the **pots forwarding-method** command in global configuration mode. To turn forwarding off, use the **no** form of this command.

pots forwarding-method {**keypad** | **functional**}

no pots forwarding-method {**keypad** | **functional**}

Syntax Description

keypad	Gives forwarding control to the Euro-ISDN switch.
functional	Gives forwarding control to the router. If you select this method, use the dual-tone multifrequency (DTMF) keypad commands listed in Table 34 to configure call-forwarding service.

Command Default

Forwarding is off

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use this command to select the type of forwarding method to be used for Euro-ISDN switches. This command does not affect any other switch types.

You can select one or more call-forwarding services at a time, but keep the following Euro-ISDN switch characteristics in mind:

- Call forward unconditional (CFU) redirects a call without restriction and takes precedence over other call-forwarding service types.
- Call forward busy (CFB) redirects a call to another number if the dialed number is busy.
- Call forward no reply (CFNR) forwards a call to another number if the dialed number does not answer within a specified period of time.

If all three call-forwarding services are enabled, CFU overrides CFB and CFNR. The default is that no call-forwarding service is selected.

If you select the functional forwarding method, use the DTMF keypad commands in Table 34 to configure the call-forwarding service.

Table 34 DTMF Keypad Commands for Call-Forwarding Service

Task	DTMF Keypad Command[1]
Activate CFU	****21***_number_**#**
Deactivate CFU	**#21#**

Table 34 DTMF Keypad Commands for Call-Forwarding Service (continued)

Task	DTMF Keypad Command[1]
Activate CFNR	****61***_number_**#**
Deactivate CFNR	**#61#**
Activate CFB	****67***_number_**#**
Deactivate CFB	**#67#**

1. Where *number* is the telephone number to which your calls are forwarded.

When you enable or disable the call-forwarding service, it is enabled or disabled for four basic services: speech, audio at 3.1 kilohertz (kHz), telephony at 3.1 kHz, and telephony at 7 kHz. You should hear a dial tone after you enter the DTMF keypad command when the call-forwarding service is successfully enabled for at least one of the four basic services. If you hear a busy tone, the command is invalid or the switch does not support that service.

Examples

The following example gives forwarding control to the router:

```
pots forwarding-method functional
```

Related Commands

Command	Description
pots prefix filter	Sets a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter.
pots prefix number	Sets a prefix to be added to a called telephone number for analog or modem calls.

pots line-type

To specify the impedance of your connected telephones, fax machines, or modems, use the **pots line-type** command in global configuration mode. To disable the specified line type, use the **no** form of this command.

pots line-type {**type1** | **type2** | **type3**}

no pots line-type {**type1** | **type2** | **type3**}

Syntax Description

type1	Runs at 600 ohms.
type2	Runs at 900 ohms.
type3	Runs at 300 or 400 ohms.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the line type to type1:

```
pots line-type type1
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots prefix filter

To set a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter, use the **pots prefix filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

pots prefix filter *number*

no pots prefix filter *number*

Syntax Description

number	Prefix filter numbers, up to a maximum of eight characters.

Command Default

No default filter is set.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 803 and Cisco 804.

Usage Guidelines

The **pots prefix filter** command is used to set a filter for prefix dialing. A maximum of ten filters can be set. Once the maximum number of filters have been configured, an additional filter is not accepted nor does it overwrite any of the existing filters.

To configure a new filter, remove at least one filter using the **no pots prefix filter** command.

You can set matching criteria for the filter using the * wildcard character. For example, if you configure the filter 1* and a dialed number starts with 1, the called number is not prefixed. Prefix filters can be of variable length. All configured prefix filters are compared to the number dialed, up to the length of the prefix filter. If there is a match, no prefix is added to the dialed number.

Examples

The following example configures five filters that prevent dial prefixes from being added to dialed numbers:

```
pots prefix filter 192
pots prefix filter 1
pots prefix filter 9
pots prefix filter 0800
pots prefix filter 08456
```

With these filters configured, a prefix is not added to the following dialed numbers:

192 Directory calls

100 Operator services

999 Emergency services

0800... Toll-free calls

08456...Calls on an Energis network information controller

Related Commands

Command	Description
pots forwarding-method	Configures the type of forwarding method to be used for Euro-ISDN (formerly NET3) switches.
pots prefix number	Sets a prefix to be added to a called telephone number for analog or modem calls.

pots prefix number

To set a prefix to be added to a called telephone number for analog or modem calls, use the **pots prefix number** command in global configuration mode. To remove the prefix, use the **no** form of this command.

pots prefix number *number*

no pots prefix number *number*

Syntax Description

number	Prefix, up to a maximum of five digits.

Command Default No prefix is associated with the called number for analog or modem calls

Command Modes Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 803 and Cisco 804.

Usage Guidelines Only one prefix can be configured using this command. If a prefix already exists, the next prefix configured with this command overwrites the old prefix. Prefixes can be of variable length, up to five digits. The **no pots prefix number** command removes the prefix.

As numbers are dialed on the keypad, a comparison is made to the configured prefix filter. When a match is determined, the number is dialed without adding the prefix. In the unlikely event that the prefix filter has more digits than the dialed number, and the dialed number matches the first digits of the prefix filter, the prefix is not added to the dialed number. For example, if the prefix filter is 5554000 and you dial 555 and stop, the router considers the called number to be 555 and does not add a prefix to the number. This event is unlikely to occur because the number of digits in dialed numbers is typically greater than the number of digits in prefix filters.

Examples The following example sets the prefix to 12345:

```
pots prefix number 12345
```

This prefix is added to any number dialed for analog or modem calls that do not match the prefix filter.

Related Commands

Command	Description
pots prefix filter	Sets a filter that prevents a dial prefix from being added to a dialed number when the digits in the dialed number match the filter.

pots ringing-freq

To specify the frequency on the Cisco 800 series router at which connected telephones, fax machines, or modems ring, use the **pots ringing-freq** command in global configuration mode. To disable the specified frequency, use the **no** form of this command.

pots ringing-freq {**20Hz** | **25Hz** | **50Hz**}

no pots ringing-freq {**20Hz** | **25Hz** | **50Hz**}

Syntax Description

20Hz	Connected devices ring at 20 Hz.
25Hz	Connected devices ring at 25 Hz.
50Hz	Connected devices ring at 50 Hz.

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the ringing frequency to 50 Hz:

```
pots ringing-freq 50Hz
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots silence-time

To specify the interval of silence after a calling party disconnects, use the **pots silence-time** command in global configuration mode. To disable the specified silence time, use the **no** form of this command.

pots silence-time *interval*

no pots silence-time *interval*

Syntax Description

interval	Number from 0 to 10 (seconds).

Command Default

The default depends on the setting of the **pots country** command. For more information, see the **pots country** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command applies to Cisco 800 series routers.

Examples

The following example sets the interval of silence to 10 seconds:

```
pots silence-time 10
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).

Command	Description
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pots tone-source

To specify the source of dial, ringback, and busy tones for your connected telephones, fax machines, or modems, use the **pots tone-source** command in global configuration mode. To disable the specified source, use the **no** form of this command.

pots tone-source {**local** | **remote**}

no pots tone-source {**local** | **remote**}

Syntax Description

local	Router supplies the tones.
remote	Telephone switch supplies the tones.

Command Default Local (router supplies the tones)

Command Modes Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines This command applies to Cisco 800 series routers.

This command applies only to ISDN lines connected to a EURO-ISDN (NET3) switch.

Examples The following example sets the tone source to remote:

```
pots tone-source remote
```

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.

Command	Description
pots distinctive-ring-guard-time	Specifies the delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
show pots status	Displays the settings of the telephone port physical characteristics and other information on the telephone interfaces on a Cisco 800 series router.

pre-dial delay

To configure a delay on an Foreign Exchange Office (FXO) interface between the beginning of the off-hook state and the initiation of dual-tone multifrequency (DTMF) signaling, use the **pre-dial delay** command in voice-port configuration mode. To reset to the default, use the **no** form of the command.

pre-dial delay *seconds*

no pre-dial delay

Syntax Description

seconds	Delay, in seconds, before signaling begins. Range is from 0 to 10. Default is 1.

Command Default 1 second

Command Modes Voice-port configuration

Command History

Release	Modification
11.(7)T	This command was introduced on the Cisco 3600 series.
12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T.

Usage Guidelines To disable the command, set the delay to 0. When an FXO interface begins to draw loop current (off-hook state), a delay is required between the initial flow of loop current and the beginning of signaling. Some devices initiate signaling too quickly, resulting in redial attempts. This command allows a signaling delay.

Examples The following example sets a predial delay value of 3 seconds on the FXO port:

```
voice-port 1/0/0
 pre-dial delay 3
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timing delay-duration	Configures delay dial signal duration for a specified voice port.

preference (dial peer)

To indicate the preferred order of a dial peer within a hunt group, use the **preference** command in dial peer configuration mode. To remove the preference, use the **no** form of this command.

preference *value*

no preference

Syntax Description

value	Integer from 0 to 10, where the lower the number, the higher the preference. Default is 0 (highest preference).

Command Default

0 (highest preference)

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was modified to support VoFR dial peers on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

This command applies to POTS, VoIP, VoFR, and VoATM dial peers.

Use this command to indicate the preference order for matching dial peers in a rotary group. Setting the preference enables the desired dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.

Note If POTS and voice-network peers are mixed in the same hunt group, the POTS dial peers must have priority over the voice-network dial peers.

Use this command with the Rotary Calling Pattern feature described in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2 chapter "Configuring H.323 Gateways."

The hunting algorithm precedence is configurable. For example, if you wish a call processing sequence to go to destination A first, to destination B second, and to destination C third, you would assign preference (0 being the highest priority) to the destinations in the following order:

- Preference 0 to A
- Preference 1 to B
- Preference 2 to C

Examples

The following example sets POTS dial peer 10 to a preference of 1, POTS dial peer 20 to a preference of 2, and VoFR dial peer 30 to a preference of 3:

```
dial-peer voice 10 pots
 destination pattern 5550150
 preference 1
 exit

dial-peer voice 20 pots
 destination pattern 5550150
 preference 2
 exit

dial-peer voice 30 vofr
 destination pattern 5550150
 preference 3
 exit
```

The following examples show different dial peer configurations:

```
Dialpeer        destpat         preference              session-target
1               4085550148      0 (highest)             jmmurphy-voip
2               408555          0                       sj-voip
3               408555          1 (lower)               backup-sj-voip
4               ..........      1                       0:D     (interface)
5               ..........      0                       anywhere-voip
```

If the destination number is 4085550148, the order of attempts is 1, 2, 3, 5, 4:

```
Dialpeer        destpat         preference
1               408555          0
2               4085550148      1
3               4085550         0
4 ..............4085550.........0
```

If the number dialed is 4085550148, the order is 2, 3, 4, 1.

Note The default behavior is that the longest matching dial peer supersedes the preference value.

Related Commands

Command	Description
called-number (dial peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.

Command	Description
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

preemption enable

To enable preemption capability on a trunk group, use the **preemption enable** command in trunk group configuration mode. To disable preemption capabilities, use the **no** form of this command.

preemption enable

no preemption enable

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the trunk group.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following command example enables preemption capabilities on trunk group test:

```
Router(config)# trunk group test
Router(config-trunk-group)# preemption enable
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption guard timer	Defines time for a DDR call and allows time to clear the last call from the channel.
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.
preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption guard timer

To define the time for a DDR call and to allow time to clear the last call from the channel, use the **preemption guard timer** command in trunk group configuration mode. To disable the preemption guard time, use the **no** form of this command.

preemption guard timer *value*

no preemption guard timer

Syntax Description

value	Number, in milliseconds for the preemption guard timer. The range is 60 to 500. The default is 60.

Command Default

No preemption guard timer is configured.

Command Modes

Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following set of commands configures a 60-millisecond preemption guard timer on the trunk group dial2.

```
Router(config)# trunk group dial2
Router(config-trunk-group)# preemption enable
Router(config-trunk-group)# preemption guard timer 60
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption level	Sets the preemption level of the selected outbound dial-peer. Voice calls can be preempted by a DDR call with higher preemption level.
preemption tone timer	Sets the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption level

To set the precedence for voice calls to be preempted by a dial-on demand routing (DDR) call for the trunk group, use the **preemption level** command in dial peer configuration mode. To restore the default preemption level setting, use the **no** form of this command

preemption level {**flash-override** | **flash** | **immediate** | **priority** | **routine**}

no preemption level

Syntax Description

flash-override	Sets the precedence for voice calls to preemption level 0 (highest).
flash	Sets the precedence for voice calls to preemption level 1.
immediate	Sets the precedence for voice calls to preemption level 2.
priority	Sets the precedence for voice calls to preemption level 3.
routine	Sets the precedence for voice calls to preemption level 4 (lowest). This is the default.

Command Default

The preemption level default is **routine** (lowest).

Command Modes

Dial peer configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following command example sets a preemption level of flash (level 1) on POTS dial-peer 20:

```
Router(config)# dial-peer voice 20 pots
Router(config-dial-peer)# preemption level flash
```

Related Commands

Command	Description
dialer preemption level	Sets the precedence for voice calls to be preempted by a DDR call for the dialer map.
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption guard timer	Defines time for a DDR call and allows time to clear the last call from the channel.
preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

preemption tone timer

To set the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call, use the **preemption tone timer** command in trunk group configuration mode. To clear the expiry time, use the **no** form of this command.

preemption tone timer *seconds*

no preemption tone timer

Syntax Description

seconds	Length of preemption tone, in seconds. Range: 4 to 30. Default: 10.

Command Default No preemption tone timer is configured.

Command Modes Trunk group configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples The following set of commands configures a 20-second preemption tone timer on trunk group dial2.

```
Router(config)# trunk group dial2
Router(config-trunk-group)# preemption enable
Router(config-trunk-group)# preemption tone timer 20
```

Related Commands

Command	Description
isdn integrate all	Enables integrated mode on an ISDN PRI interface.
max-calls	Sets the maximum number of calls that a trunk group can handle.
preemption enable	Enables preemption capabilities on a trunk group.
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.

prefix

To specify the prefix of the dialed digits for a dial peer, use the **prefix** command in dial peer configuration mode. To disable this feature, use the **no** form of this command.

prefix *string*

no prefix

Syntax Description

string	Integers that represent the prefix of the telephone number associated with the specified dial peer. Valid values are 0 through 9 and a comma (,). Use a comma to include a pause in the prefix.

Command Default Null string

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)XJ	This command was implemented on the Cisco AS5300. It and modified for store-and-forward fax.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.

Usage Guidelines Use this command to specify a prefix for a specific dial peer. When an outgoing call is initiated to this dial peer, the **prefix** *string* value is sent to the telephony interface first, before the telephone number associated with the dial peer.

If you want to configure different prefixes for dialed numbers on the same interface, you need to configure different dial peers.

This command is applicable only to plain old telephone service (POTS) dial peers. This command applies to off-ramp store-and-forward fax functions.

Examples

The following example specifies a prefix of 9 and then a pause:

```
dial-peer voice 10 pots
 prefix 9,
```

The following example specifies a prefix of 5120002:

```
Router(config-dial-peer)# prefix 5120002
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
destination-pattern	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

prefix (Annex G)

To restrict the prefixes for which the gatekeeper should query the Annex G border element (BE), use the **prefix** command in gatekeeper border element configuration mode.

prefix *prefix** [**seq** | **blast**]

Syntax Description

*prefix**	Prefix for which BEs should be queried.
seq	(Optional) Queries are sent out to the neighboring BEs sequentially.
blast	(Optional) Queries are sent out to the neighboring BEs simultaneously.

Command Default

Any time a remote zone query occurs, the BE is also queried.

Command Modes

Gatekeeper border element configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

By default, the gatekeeper sends all remote zone requests to the BE. Use this command only if you want to restrict the queries to the BE to a specific prefix or set of prefixes.

Examples

The following example directs the gatekeeper to query the BE using a prefix of 408.

```
Router(config-gk-annexg)# prefix 408* seq
```

Related Commands

Command	Description
h323-annexg	Enables the BE on the gatekeeper and enters border element configuration mode.

prefix (stcapp-fac)

To designate a prefix string to precede the dialing of SCCP telephony control (STC) feature access codes, use the **prefix** command in STC application feature access-code configuration mode. To return the prefix to its default, use the **no** form of this command.

prefix *prefix-string*

no prefix

Syntax Description

prefix-string	String of one to ten characters that can be dialed on a telephone keypad. String must start with * (asterisk) or # (pound sign). Default is **.

Command Default

The default prefix is ** (two asterisks).

Command Modes

STC application feature access-code configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the STC application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Phone users dial the feature access code (FAC) prefix string before dialing a FAC that activates a feature. For example, to set call forwarding for all calls using the default prefix and FAC, a phone user dials **1.

Use this command only if you want to change the prefix from its default (**).

The **show running-config** command displays nondefault FACs and prefixes only. The **show stcapp feature codes** command displays all FACs and prefixes.

Examples

The following example sets a FAC prefix of two pound signs (##). After this value is configured, a phone user dials ##2 on the keypad to forward all calls for that extension.

```
Router(config)# stcapp feature access-code
Router(stcapp-fac)# prefix ##
Router(stcapp-fac)# call forward all 2
Router(stcapp-fac)# call forward cancel 3
Router(stcapp-fac)# pickup local 6
Router(stcapp-fac)# pickup group 5
Router(stcapp-fac)# pickup direct 4
Router(stcapp-fac)# exit
```

Related Commands

Command	Description
call forward all	Designates an STC application feature access code to activate the forwarding of all calls.
call forward cancel	Designates an STC application feature access code to cancel the forwarding of all calls.
pickup direct	Designates an STC application feature access code for directed call pickup.
pickup group	Designates an STC application feature access code for group call pickup from another group.
pickup local	Designates an STC application feature access code for group call pickup from the local group.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature access codes.
stcapp feature access-code	Enters STC application feature access-code configuration mode to set feature access codes.

prefix (stcapp-fsd)

To designate a prefix string to precede the dialing of SCCP telephony control (STC) application feature speed-dial codes, use the **prefix** command in STC application feature speed-dial configuration mode. To return the prefix to its default, use the **no** form of this command.

prefix *prefix-string*

no prefix

Syntax Description

prefix-string	String of one to ten characters that can be dialed on a telephone keypad. String must start with * (asterisk) or # (pound sign). Default is *.

Command Default

The default prefix is * (one asterisk).

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the STC application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Phone users dial the feature speed-dial (FSD) prefix string before dialing an FSD code that dials a telephone number. For example, to dial the telephone number that is stored in speed-dial position 2, a phone user dials *2.

Use this command only if you want to change the prefix from its default (*).

The **show running-config** command displays nondefault FSDs and prefixes only. The **show stcapp feature codes** command displays all feature speed-dial FSDs and prefixes.

Examples

The following example sets an FSD prefix of three asterisks (***). After this value is configured, a phone user presses ***2 on the keypad to dial speed-dial number 2.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ***
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# redial 9
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show stcapp feature codes	Displays configured and default STC application feature access codes.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

preloaded-route

To enable preloaded route support for VoIP Session Initiation Protocol (SIP) calls, use the **preloaded-route** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

preloaded-route [**sip-server**] **service-route**

no preloaded-route

Syntax Description

sip-server	(Optional) Adds SIP server information to the Route header.
service-route	Adds the Service-Route information to the Route header.

Command Default

Route support is not enabled.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class preloaded-route** command, in dial-peer configuration mode, takes precedence over the **preloaded-route** command in SIP configuration mode. However, if the **voice-class preloaded-route** command is configured with the **system** keyword, the gateway uses the global settings configured by the **preloaded-route** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example shows how to configure the system to include SIP server and Service-Route information in the Route header:

```
voice service voip
sip
 preloaded-route sip-server service-route
```

The following example shows how to configure the system to include only Service-Route information in the Route header:

```
voice service voip
sip
 preloaded-route service-route
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class preloaded-route	Enables preloaded route support for dial-peer SIP calls.

presence

To enable presence service and enter presence configuration mode, use the **presence** command in global configuration mode. To disable presence service, use the **no** form of this command.

presence

no presence

Syntax Description This command has no arguments or keywords.

Command Default Presence service is disabled.

Command Modes Global configuration (config)

Command History

Release	Cisco Product	Modification
12.4(11)XJ	Cisco Unified CME 4.1	This command was introduced.
12.4(15)T	Cisco Unified CME 4.1	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines This command enables the router to perform the following presence functions:

- Process presence requests from internal lines to internal lines. Notify internal subscribers of any status change.
- Process incoming presence requests from a SIP trunk for internal lines. Notify external subscribers of any status change.
- Send presence requests to external presentities on behalf of internal lines. Relay status responses to internal lines.

Examples The following example shows how to enable presence and enter presence configuration mode to set the maximum subscriptions to 150:

```
Router(config)# presence
Router(config-presence)# max-subscription 150
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
debug presence	Displays debugging information about the presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.

Command	Description
presence enable	Allows the router to accept incoming presence requests.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

presence call-list

To enable Busy Lamp Field (BLF) monitoring for call lists and directories on phones registered to the Cisco Unified CME router, use the **presence call-list** command in ephone, presence, or voice register pool configuration mode. To disable BLF indicators for call lists, use the **no** form of this command.

presence call-list

no presence call-list

Syntax Description

This command has no arguments or keywords.

Command Default

BLF monitoring for call lists is disabled.

Command Modes

Ephone configuration (config-ephone)
Presence configuration (config-presence)
Voice register pool configuration (config-register pool)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command enables a phone to monitor the line status of directory numbers listed in a directory or call list, such as a missed calls, placed calls, or received calls list. Using this command in presence mode enables the BLF call-list feature for all phones. To enable the feature for an individual SCCP phone, use this command in ephone configuration mode. To enable the feature for an individual SIP phone, use this command in voice register pool configuration mode.

If this command is disabled globally and enabled in voice register pool or ephone configuration mode, the feature is enabled for that voice register pool or ephone.

If this command is enabled globally, the feature is enabled for all voice register pools and ephones regardless of whether it is enabled or disabled on a specific voice register pool or ephone.

To display a BLF status indicator, the directory number associated with a telephone number or extension must have presence enabled with the **allow watch** command.

For information on the BLF status indicators that display on specific types of phones, see the Cisco Unified IP Phone documentation for your phone model.

Examples

The following example shows the BLF call-list feature enabled for ephone 1. The line status of a directory number that appears in a call list or directory is displayed on phone 1 if the directory number has presence enabled.

```
Router(config)# ephone 1
Router(config-ephone)# presence call-list
```

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
presence	Enables presence service and enters presence configuration mode.
show presence global	Displays configuration information about the presence service.

presence enable

To allow incoming presence requests, use the **presence enable** command in SIP user-agent configuration mode. To block incoming requests, use the **no** form of this command.

presence enable

no presence enable

Syntax Description This command has no arguments or keywords.

Command Default Incoming presence requests are blocked.

Command Modes SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines This command allows the router to accept incoming presence requests (SUBSCRIBE messages) from internal watchers and SIP trunks. It does not impact outgoing presence requests.

Examples The following example shows how to allow incoming presence requests:

```
Router(config)# sip-ua
Router(config-sip-ua)# presence enable
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

pri-group (pri-slt)

To specify an ISDN PRI on a channelized T1 or E1 controller, use the **pri-group** (pri-slt) command in controller configuration mode. To remove the ISDN PRI configuration, use the **no** form of this command.

pri-group [**timeslots** *timeslot-range* [**nfas_d** [**backup** | **none** | **primary** [**nfas_int** *number*]] [**nfas-group** *number* [**iua** *as-name*]]]

no pri-group

Syntax Description

timeslots *timeslot-range*	Specifies a single range of timeslot values in the PRI goup. For T1, the allowable range is from 1 to 23. For E1, the allowable range is from 1 to 31.
nfas_d	Specifies the operation of the D channel timeslot.
backup	(Optional) Specifes that the operation of the D channel timeslot on this controller is the NFAS D backup.
none	(Optional) Specifes that the D channel timeslot is used as an additional B channel.
primary	Specifies that the D channel timeslot on this controller in NFAS D.
nfas_int *range*	Specifies the provisioned NFAS interface value. Valid values range from 0 to 32.
nfas-group *number*	Specifies the NFAS group and the NFAS group number. Valid values range from 0 to 31.
iua *as-name*	Binds the Non-Facility Associated Signaling (NFAS) group to the IDSN User Adaptation Layer (IUA) application server (AS).

Command Default No ISDN-PRI group is configured.

Command Modes Controller configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(15)T	This command was integrated on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

The pri-group (pri-slt) command provides another way to bind a D channel to a specific IUA AS. This option allows the RLM group to be configured at the pri-group level instead of in the D channel configuration. For example, a typical configuration would look like the following:

```
controller t1 1/0/0
 pri-group timeslots 1-24 nfas_d pri nfas_int 0 nfas_group 1 iua asname
```

Before you enter the **pri-group** command, you must specify an ISDN-PRI switch type and an E1 or T1 controller.

When configuring NFAS, you use an extended version of the **pri-group** command to specify the following values for the associated channelized T1 controllers configured for ISDN:

- The range of PRI timeslots to be under the control of the D channel (timeslot 24).
- The function to be performed by timeslot 24 (primary D channel, backup, or none); the latter specifies its use as a B channel.
- The group identifier number for the interface under the control of a particular D channel.

The **iua** keyword is used to bind an NFAS group to the IUA AS.

When binding the D channel to an IUA AS, the *as-name* must match the name of an AS set up during IUA configuration.

Before you can modify a PRI group on a Media Gateway Controller (MGC), you must first shut down the D channel.

The following shows how to shut down the D channel:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface Dchannel3/0:1
Router(config-if)# shutdown
```

Examples

The following example configures the NFAS primary D channel on one channelized T1 controller, and binds the D channel to an IUA AS. This example uses the Cisco AS5400 and applies to T1, which has 24 timeslots and is used mainly in North America and Japan:

```
Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1
iua as5400-4-1
```

The following example applies to E1, which has 32 timeslots and is used by the rest of the world:

```
Router(config-controller)# pri-group timeslots 1-31 nfas-d primary nfas-int 0 nfas-group 1
iua as5400-4-1
```

The following example configures ISDN-PRI on all time slots of controller E1:

```
Router(config)# controller E1 4/1
Router(config-controller)# pri-group timeslots 1-7,16
```

In the following example, the **rlm-timeslot** keyword automatically creates interface serial 4/7:11 (4/7:0:11 if you are using the CT3 card) for the D channel object on a Cisco AS5350. You can choose any timeslot other than 24 to be the virtual container for the D channel parameters for ISDN.

```
Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 0
rlm-timeslot 3
```

Related Commands

Command	Description
isdn switch-type	Configures the Cisco 2600 series router PRI interface to support QSIG signaling.

pri-group nec-fusion

To configure your NEC PBX to support Fusion Call Control Signaling (FCCS), use the **pri-group nec-fusion** command in controller configuration mode. To disable FCCS, use the **no** form of this command.

pri-group nec-fusion {*pbx-ip-address* | *pbx-ip-host-name*} **pbx-port** *number*

no pri-group nec-fusion {*pbx-ip-address* | *pbx-ip-host-name*} **pbx-port** *number*

Syntax Description

pbx-ip-address	IP address of the NEC PBX.
pbx-ip-host-name	Host name of the NEC PBX.
pbx-port *number*	Port number for the PBX. Range is from 49152 to 65535. Default is 55000. If this value is already in use, the next greater value is used.

Command Default

PBX port number: 55000

Command Modes

Controller configuration

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.2(1)	This command was modified to add support for setup messages from a POTS dial peer.

Usage Guidelines

This command is used only if the PBX in your configuration is an NEC PBX, and if you are configuring it to run FCCS and not QSIG signaling.

Examples

The following example directs this NEC PBX to use FCCS:

```
pri-group nec-fusion 172.31.255.255 pbx-port 60000
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support QSIG signaling.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

pri-group timeslots

To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN PRI signaling time slot, use the **pri-group timeslots** command in controller configuration mode. To remove or change the ISDN PRI configuration, use the **no** form of this command.

pri-group timeslots *timeslot-range* [**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [**iua** *as-name* | **rlm-group** *number* | **service mgcp**]} | **service mgcp**]

no pri-group timeslots *timeslot-range* [**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [**iua** *as-name* | **rlm-group** *number* | **service mgcp**]} | **service mgcp**]

Syntax Description

timeslot-range	A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range. **Note** Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.
nfas_d	(Optional) Configures the operation of the ISDN PRI D channel.
backup	The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.
none	The D-channel time slot is used as an additional B channel.
primary	The D-channel time slot is used as the NFAS D primary.
nfas_int *number*	Specifies the provisioned NFAS interface as a value. Valid values for the NFAS interface range from 0 to 44.
nfas_group *number*	Specifies the NFAS group. Valid values for the NFAS group number range from 0 to 31.
iua *as-name*	(Optional) Configures the ISDN User Adaptation Layer (IUA) application server (AS) name.
rlm-group *number*	(Optional) Specifies the Redundant Link Manager (RLM) group and releases the ISDN PRI signaling channel. Valid values for the RLM group number range from 0 to 255.
service mgcp	(Optional) Configures the service type as Media Gateway Control Protocol (MGCP) service.

Defaults

No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (**primary-ni** keyword) when the **pri-group timeslots** command is configured with the **rlm-group** subkeyword.

Command Modes

Controller configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3	This command was enhanced to support NFAS.
12.0(2)T	This command was implemented on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)B	This command was modified with the **rlm-group** subkeyword to support release of the ISDN PRI signaling channels.
12.2(15)T	The modifications in Cisco IOS Release 12.2(8)B were integrated into Cisco IOS Release 12.2(15)T.
12.4(16)b	This command was modified to ensure that the NFAS primary interface is configured before the NFAS backup or NFAS none interfaces are configured.
12.4(24)T	Support was extended to provide backup functionality for the NFAS interface in MGCP backhaul mode. With this support, if the primary fails, backup can become active and calls can be maintained.

Usage Guidelines

The **pri-group** command supports the use of DS0 time slots for Signaling System 7 (SS7) links, and therefore the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 span. In these configurations, the command applies to voice applications.

In SS7-enabled Voice over IP (VoIP) configurations when an RLM group is configured, High-Level Data Link Control (HDLC) resources allocated for ISDN signaling on a digital subscriber line (DSL) interface are released and the signaling slot is converted to a bearer channel (B24). The D channel will be running on IP. The chosen D-channel time slot can still be used as a B channel by using the **isdn rlm-group** interface configuration command to configure the NFAS groups.

NFAS allows a single D channel to control multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees one B channel on each interface to carry other traffic. A backup D channel can also be configured for use when the primary NFAS D channel fails. When a backup D channel is configured, any hard system failure causes a switchover to the backup D channel and currently connected calls remain connected.

NFAS is supported only with a channelized T1 controller and, as a result, must be ISDN PRI capable. When the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all members of the associated NFAS group. Any configuration changes made to the primary D channel will be propagated to all NFAS group members. The primary D channel interface is the only interface shown after the configuration is written to memory.

The channelized T1 controllers on the router must also be configured for ISDN. The router must connect to either an AT&T 4ESS, Northern Telecom DMS-100 or DMS-250, or National ISDN switch type.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should be the same configuration as that configured on the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

You can disable a specified channel or an entire PRI interface, thereby taking it out of service or placing it into one of the other states that is passed in to the switch using the **isdn service** interface configuration command.

In the event that a controller belonging to an NFAS group is shut down, all active calls on the controller that is shut down will be cleared (regardless of whether the controller is set to primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (In service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

The expected behavior in NFAS when an ISDN D channel (serial interface) is shut down is that ISDN Layer 2 should go down but keep ISDN Layer 1 up, and that the entire interface will go down after the amount of seconds specified for timer T309.

Note The active D channel changeover between primary and backup controllers happens only when one of the link fails and not when the link comes up. The T309 timer is triggered when the changeover takes place.

Note You must first configure the NFAS primary D channel before configuring the NFAS backup or NFAS none interfaces. If this order is not followed, this message is displayed:

"NFAS backup and none interfaces are not allowed to be configured without primary. First configure primary D channel."

To remove the NFAS primary D channel after the NFAS backup or NFAS none interfaces are configured, you must remove the NFAS backup or NFAS none interfaces first, and then remove the NFAS primary D channel.

Examples

The following example configures T1 controller 1/0 for PRI and for the NFAS primary D channel. This primary D channel controls all the B channels in NFAS group 1.

```
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

The following example specifies ISDN PRI on T1 slot 1, port 0, and configures voice and data bearer capability on time slots 2 through 6:

```
isdn switch-type primary-4ess
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 2-6
```

The following example configures a standard ISDN PRI interface:

```
! Standard PRI configuration:
controller t1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit

! Standard ISDN serial configuration:
interface serial1:23
! Set ISDN parameters:
 isdn T309 4000
 exit
```

The following example configures a dedicated T1 link for SS7-enabled VoIP:

```
controller T1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit

! In a dedicated configuration, we assume the 24th timeslot will be used by ISDN.
! Serial interface 0:23 is created for configuring ISDN parameters.
interface Serial:24
! The D channel is on the RLM.
 isdn rlm 0
 isdn  T309 4000
 exit
```

The following example configures a shared T1 link for SS7-enabled VoIP. The **rlm-group 0** portion of the **pri-group timeslots** command releases the ISDN PRI signaling channel.

```
controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
 end

! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
 end
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
interface Dchannel	Specifies an ISDN D-channel interface for VoIP applications that require release of the ISDN PRI signaling time slot for RLM configurations.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI signaling.
isdn rlm-group	Specifies the RLM group number that ISDN will start using.
isdn switch-type	Specifies the central office switch type on the ISDN PRI interface.
isdn timer t309	Changes the value of the T309 timer to clear network connections and release the B channels when there is no signaling channel active, that is, when the D channel has failed and cannot recover by switching to an alternate D channel. Calls remain active and able to transfer data when the D channel fails until the T309 timer expires. The T309 timer is canceled when D-channel failover succeeds.
show isdn nfas group	Displays all the members of a specified NFAS group or all NFAS groups.

primary (gateway accounting file)

To set the primary location for storing the call detail records (CDRs) generated for file accounting, use the **primary** command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

primary {**ftp** *path/filename* **username** *username* **password** *password* | **ifs** *device*:*filename*}

no primary {**ftp** | **ifs**}

Syntax Description

ftp *path/filename*	Name and location of the file on an external FTP server. Filename is limited to 25 characters.
ifs *device*:*filename*	Name and location of the file in flash memory or other internal file system on this router. Values depend on storage devices available on the router, for example flash or slot0. Filename is limited to 25 characters.
username *username*	User ID for authentication.
password *password*	Password user enters for authentication.

Command Default

Call records are saved to **flash:cdr**.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the name and location of the primary file where CDRs are stored during the file accounting process. The filename you assign is appended with the gateway hostname and time stamp at the time the file is created to make the filename unique.

For example, if you specify the filename cdrtest1 on a router with the hostname cme-2821, a file is created with the name cdrtest1.cme-2821.2007_10_28T22_21_41.000, where 2007_10_28T22_21_41.000 is the time that the file was created.

Limit the filename you assign with this command to 25 characters, otherwise it could be truncated when the accounting file is created because the full filename, including the appended hostname and timestamp, is limited to 63 characters.

If the file transfer to this primary device fails, the file accounting process retries the primary device up to the number of times defined by the **maximum retry-count** command and then switches over to the secondary device defined with the **secondary** command.

To manually switch back to the primary device when it becomes available, use the **file-acct reset** command. The system does not automatically switch back to the primary device.

A syslog warning message is generated when flash becomes full.

Examples

The following example shows the primary location of the accounting file is set to an external FTP server and the filename is cdrtest1:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary flash ifs:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

The following examples show how the accounting file is named when it is created. The router hostname and time stamp are appended to the filename that you assign with this command:

```
cme-2821(config)# primary ftp server1/cdrtest1 username bob password temp
```

The name of the accounting file that is created has the following format:

cdrtest1.cme-2821.06_04_2007_18_44_51.785

Related Commands

Command	Description
file-acct flush	Manually flushes the CDRs from the buffer to the accounting file.
file-acct reset	Manually switches back to the primary device for file accounting.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

privacy

To set privacy support at the global level as defined in RFC 3323, use the **privacy** command in voice service voip sip configuration mode. To remove privacy support as defined in RFC 3323, use the **no** form of this command.

privacy {**pstn** | *privacy-option* [**critical**]}

no privacy

Syntax Description

pstn	Requests that the privacy service implements a privacy header using the default Public Switched Telephone Network (PSTN) rules for privacy (based on information in Octet 3a). When selected, this becomes the only valid option.
privacy-option	The privacy support options to be set at the global level. The following keywords can be specified for the *privacy-option* argument: • **header** — Requests that privacy be enforced for all headers in the Session Initiation Protocol (SIP) message that might identify information about the subscriber. • **history** — Requests that the information held in the history-info header is hidden outside the trust domain. • **id** — Requests that the Network Asserted Identity that authenticated the user be kept private with respect to SIP entities outside the trusted domain. • **session** — Requests that the information held in the session description is hidden outside the trust domain. • **user** — Requests that privacy services provide a user-level privacy function. **Note** The keywords can be used alone, altogether, or in any combination with each other, but each keyword can be used only once.
critical	(Optional) Requests that the privacy service performs the specified service or fail the request. **Note** This optional keyword is only available after at least one of the *privacy-option* keywords (**header**, **history**, **id**, **session**, or **user**) has been specified and can be used only once per command.

Command Default Privacy support is disabled.

Command Modes Voice service voip sip configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	The **history** keyword was added to provide support for the history-info header information.

Usage Guidelines

Use the **privacy** command to instruct the gateway to add a Proxy-Require header set to a value supported by RFC 3323 in outgoing SIP request messages.

Use the **privacy critical** command to instruct the gateway to add a Proxy-Require header with the value set to critical. If a user agent sends a request to an intermediary that does not support privacy extensions, the request fails.

Examples

The following example shows how to set the privacy to PSTN:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy pstn
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAI or PPI privacy headers in outgoing SIP requests or response messages.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.
clid (voice-service-voip)	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, removes the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allows a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers.
voice-class sip privacy	Sets privacy support at the dial-peer configuration level as defined in RFC 3323.

privacy (supplementary-service)

To prevent phones on a shared line from joining active calls, use the **privacy** command in supplementary-service voice-port configuration mode. To return to the default behavior, use the **no** form of this command.

privacy {**on** | **off**}

no privacy

Syntax Description

on	Prevents other phones on the shared line to join active calls.
off	Allows other phones on the shared line to join active calls.

Command Default

The **no privacy** command implies that a port does not decide on its privacy status. It is not the gateway but the Cisco Unified CM that decides on the privacy status of a port.

Command Modes

Supplementary-service voice-port configuration mode (config-stcapp-suppl-serv-port)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **privacy** command enables privacy support on analog endpoints that are connected to Foreign Exchange Station (FXS) ports on a Cisco IOS Voice Gateway, such as a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway.

Use the **privacy** command to prevent other phones on the shared line to join active calls.

Examples

The following example shows how to turn on privacy support on port 2/4 on a Cisco VG224:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/4
Router(config-stcapp-suppl-serv-port)# privacy on
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

privacy-policy

To configure the privacy header policy options at the global level, use the **privacy-policy** command in voice service VoIP SIP configuration mode. To disable privacy header policy options, use the **no** form of this command.

privacy-policy {**passthru** | **send-always** | **strip** {**diversion** | **history-info**}}

no privacy-policy {**passthru** | **send-always** | **strip** { **diversion** | **history-info**}}

Syntax Description

passthru	Passes the privacy values from the received message to the next call leg.
send-always	Passes a privacy header with a value of None to the next call leg, if the received message does not contain privacy values but a privacy header is required.
strip	Strips the diversion or history-info headers received from the next call leg.
diversion	Strips the diversion headers received from the next call leg.
history-info	Strips the history-info headers received from the next call leg.

Command Default

No privacy-policy settings are configured.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **strip**, **diversion**, and **history-info** keywords were added.

Usage Guidelines

If a received message contains privacy values, use the **privacy-policy passthru** command to ensure that the privacy values are passed from one call leg to the next. If the received message does not contain privacy values but the privacy header is required, use the **privacy-policy send-always** command to set the privacy header to None and forward the message to the next call leg. If you want to strip the diversion and history-info from the headers received from the next call leg, use the **privacy-policy strip** command. You can configure the system to support all the options at the same time.

Examples

The following example shows how to enable the pass-through privacy policy:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy passthru
```

The following example shows how to enable the send-always privacy policy:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy send-always
```

The following example shows how to enable the strip privacy policy:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy strip diversion
Router(conf-serv-sip)# privacy-policy strip history-info
```

The following example shows how to enable the pass-through, send-always privacy, and strip policies:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# privacy-policy passthru
Router(conf-serv-sip)# privacy-policy send-always
Router(conf-serv-sip)# privacy-policy strip diversion
Router(conf-serv-sip)# privacy-policy strip history-info
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAID or PPID privacy headers in outgoing SIP requests or response messages.
voice-class sip privacy-policy	Configures the privacy header policy options at the dial-peer configuration level.

progress_ind

To configure an outbound dial peer on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE) to override and remove or replace the default progress indicator (PI) in specified call messages, use the **progress_ind** command in dial peer voice configuration mode. To disable removal or replacement of the default PI in specific call messages, use the **no** form of this command.

progress_ind {{**alert** | **callproc**} {**enable** *pi-number* | **disable** | **strip** [*strip-pi-number*]} | {**connect** | **disconnect** | **progress** | **setup**} {**enable** *pi-number* | **disable**}}

no progress_ind {**alert** | **callproc** | **connect** | **disconnect** | **progress** | **setup**}

Syntax Description

alert	Specifies that the configuration applies to call Alert messages.
callproc	Specifies that the configuration applies to Session Initiation Protocol (SIP) 183 Session In Progress (Call_Proceeding) messages.
connect	Specifies that the configuration applies to call Connect messages.
disconnect	Specifies that the configuration applies to call Disconnect messages.
progress	Specifies that the configuration applies to call Progress messages.
setup	Specifies that the configuration applies to call Setup messages.
enable	Enables user-specified configuration of the progress indicator on the specified call message type.
pi-number	Specifies the PI to be used in place of the default PI. The following are acceptable PI values according to the call message type: • Alert, Connect, Progress, and SIP 183 Session In Progress messages: 1, 2, or 8. • Disconnect messages: 8. • Setup messages: 0, 1, or 3.
disable	Disables user-specified configuration of the progress indicator on the specified call message type.
strip	Configures the dial peer to remove all or specific progress indicators in the specified call message type. **Note** This option applies only to call Alert message on POTS dial peers or to call Proceeding messages on VoIP dial peers.
strip-pi-number	(optional) Specifies that only a specific PI is to be removed from the specified call message. The value can be 1, 2, or 8.

Command Default

This command is disabled on the outbound dial peer and the default progress indicator received in the incoming call message is passed intact (it is not intercepted, modified, or removed).

Command Modes

Dial peer voice configuration (conf-dial-peer)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco 7500 series, Cisco MC3810, Cisco AS5300, and Cisco AS5800.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(1)	This command was modified. Support was added for setup messages from a POTS dial peer.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
15.0(1)XA	This command was modified. Support was added for stripping of PIs in call Alert and SIP 183 Session In Progress (Call_Proceeding) messages.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.

Usage Guidelines

Before configuring the **progress_ind** command on an outbound dial peer, you must configure a destination pattern on the dial peer. To configure a destination pattern for an outbound dial peer, use the **destination-pattern** command in dial peer voice configuration mode. Once you have set a destination pattern on the dial peer, you can then use the **progress_ind** command, also in dial peer voice configuration mode, to override and replace or remove the default PI in specific call message types.

You can use the **progress_ind** command to configure replacement behavior on outbound dial peers on a Cisco IOS voice gateway or Cisco UBE to ensure proper end-to-end signaling of VoIP calls. You can also use this command to configure removal (stripping) of PIs on outbound dial peers on Cisco IOS voice gateways or Cisco UBEs, such as when configuring a Cisco IOS SIP gateway (or SIP-SIP Cisco UBE) to not generate additional SIP 183 Session In Progress messages.

For messages that contain multiple PIs, behavior configured using the **progress_ind** command will override only the first PI in the message. Additionally, configuring a replacement PI will not result in an override of the default PI in call Progress messages if the Progress message is sent after a backward cut-through event, such as when an Alert message with a PI of 8 was sent before the Progress message.

Use the **no progress_ind** command in dial peer voice configuration mode to disable PI override configurations on a dial peer on a Cisco IOS voice gateway or Cisco UBE.

Examples

The following example shows how to configure POTS dial peer 3 to override default PIs in call Progress and Connect messages and replace them with a PI of 1:

```
Router(config)# dial-peer voice 3 pots
Router(config-dial-peer)# destination-pattern 555
Router(config-dial-peer)# progress_ind progress enable 1
Router(config-dial-peer)# progress_ind connect enable 1
```

The following example configures outbound VoIP dial peer 1 to override SIP 183 Session In Progress messages and to strip out any PIs with a value of 8:

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# destination-pattern 777
Router(config-dial-peer)# progress_ind callproc strip 8
```

Related Commands

Command	Description
destination-pattern	Specifies the destination pattern (prefix or full E.164 telephone number) to be used on an outbound dial peer.

protocol mode

To configure the Cisco IOS Session Initiation Protocol (SIP) stack, use the **protocol mode** command in SIP user-agent configuration mode. To disable the configuration, use the **no** form of this command.

protocol mode {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}

no protocol mode

Syntax Description

ipv4	Specifies the IPv4-only mode.
ipv6	Specifies the IPv6-only mode.
dual-stack	Specifies the dual-stack (that is, IPv4 and IPv6) mode.
preference {**ipv4** | **ipv6**}	(Optional) Specifies the preferred dual-stack mode, which can be either IPv4 (the default preferred dual-stack mode) or IPv6.

Command Default

No protocol mode is configured.
The Cisco IOS SIP stack operates in IPv4 mode when the **no protocol mode** or **protocol mode ipv4** command is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

The **protocol mode** command is used to configure the Cisco IOS SIP stack in IPv4-only, IPv6-only, or dual-stack mode. For dual-stack mode, the user can (optionally) configure the preferred family, IPv4 or IPv6.

For a particular mode (for example, IPv6-only), the user can configure any address (for example, both IPv4 and IPv6 addresses) and the system will not hide or restrict any commands on the router. SIP chooses the right address for communication based on the configured mode on a per-call basis.

For example, if the domain name system (DNS) reply has both IPv4 and IPv6 addresses and the configured mode is IPv6-only (or IPv4-only), the system discards all IPv4 (or IPv6) addresses and tries the IPv6 (or IPv4) addresses in the order they were received in the DNS reply. If the configured mode is dual-stack, the system first tries the addresses of the preferred family in the order they were received in the DNS reply. If all of the addresses fail, the system tries addresses of the other family.

Examples

The following example configures dual-stack as the protocol mode:

```
Router(config-sip-ua)# protocol mode dual-stack
```

The following example configures IPv6 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv6
```

The following example configures IPv4 only as the protocol mode:

```
Router(config-sip-ua)# protocol mode ipv4
```

The following example configures no protocol mode:

```
Router(config-sip-ua)# no protocol mode
```

Related Commands

Command	Description
sip ua	Enters SIP user-agent configuration mode.

protocol rlm port

To configure the RLM port number, use the **protocol rlm port** RLM configuration command. To disable this function, use the **no** form of this command.

protocol rlm port *port-number*

no protocol rlm port *port-number*

Syntax Description

port-number	RLM port number. See Table 35 for the port number choices.

Command Default

3000

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

The port number for the basic RLM connection can be reconfigured for the entire RLM group. Table 35 lists the default RLM port numbers.

Table 35 Default RLM Port Number

Protocol	Port Number
RLM	3000
ISDN	Port[RLM]+1

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.

Command	Description
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

proxy h323

To enable the proxy feature on your router, use the **proxy h323** command in global configuration mode. To disable the proxy feature, use the **no** form of this command.

proxy h323

no proxy h323

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.

Usage Guidelines If the multimedia interface is not enabled using this command or if no gatekeeper is available, starting the proxy allows it to attempt to locate these resources. No calls are accepted until the multimedia interface and the gatekeeper are found.

Examples The following example turns on the proxy feature:

```
proxy h323
```

Cisco IOS Voice Commands: Q

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

q850-cause

To map a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code, use the **q850-cause** command in application-map configuration mode. To disable the code-to-code mapping, use the **no** form of this command.

q850-cause *code-id* **q850-cause** *code-id*

no q850-cause *code-id* **q850-cause** *code-id*

Syntax Description

code-id	Q.850 call-disconnect cause code to be mapped. Range: 1 to 127.

Command Default

No mapping occurs.

Command Modes

Application-map

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to map a Q.850 call-disconnect cause code to any different Q.850 call-disconnect cause code.

Use this command in conjunction with the **application** and **map** commands.

This command operates only on incoming H.323 call legs that are disconnected by a call-control application.

Examples

The following example maps cause code 34 to cause code 17:

```
Router(config)# application
Router(config-app)# map
Router(config-app-map)# q850-cause 34 q850-cause 17
```

Related Commands

Command	Description
application	Enables a specific application on a dial peer.
map	Enables mapping.
map q850-cause	Maps a Q.850 call-disconnect cause code to a tone.
progress_ind	Sets a specific progress indicator in Call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

qsig decode

To enable decoding for QSIG supplementary services, use the **qsig decode** command in voice service configuration mode. To reset to the default, use the **no** form of this command.

qsig decode

no qsig decode

Syntax Description This command has no keywords or arguments.

Command Default QSIG decoding is disabled.

Command Modes Voice service configuration

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines This command decodes application protocol data units (APDUs) for supplementary services. If this command is not enabled, data units are not interpreted and are tunneled through the router.

Examples The following example enables QSIG decoding:

```
Router(config)# voice service voip
Router(conf-voi-serv)# qsig decode
```

Related Commands

Command	Description
supplementary-service h450.7	Globally enables H.450.7 supplementary services capabilities exchange.

query-interval

To configure the interval at which the local border element (BE) queries the neighboring BE, use the **query-interval** command in Annex G Neighbor BE Configuration mode. To remove the interval, use the **no** form of this command.

query-interval *query-interval*

no query-interval

Syntax Description

query-interval	Frequency, in minutes, at which this BE should query the specified neighbor BE for descriptors. Default is 30. A value of 0 disables periodic querying.

Defaults

30 minutes

Command Modes

Annex G Neighbor BE configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to configure the interval at which the local BE queries the neighboring BE. Use this command only if you want a query interval other than 30 minutes.

Examples

The following example sets the query interval to 45 minutes:

```
Router(config-annexg-neigh)# query-interval 45
```

Related Commands

Command	Description
emulate	Configures the local BE to cache the descriptors received from its neighbors. If caching is enabled, the neighbors are queried at the specified interval for their descriptors.
local	Configures the identifier for the neighbor BE.
session transport	Configures the neighbor's port number that is used for exchanging Annex G messages.

Cisco IOS Voice Commands: R

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6** command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}

no radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. **Note** The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include "Service-Type=Outbound" as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice *value*	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Command Default

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **mandatory** keyword was added.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in an Access-Accept packet containing multiple instances being treated as though an Access-Reject was received.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router(config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router(config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router(config)# radius-server attribute 6 voice 1
```

rai target

To configure the Session Initiation Protocol (SIP) Resource Allocation Indication (RAI) mechanism, use the **rai target** command in SIP UA configuration mode. To disable SIP RAI configuration, use the **no** form of this command.

rai target *target-address* **resource-group** *group-index* [**transport** [**tcp** [**tls** [**scheme** {**sip** | **sips**}]] | **udp**]]

no rai target *target-address*

Syntax Description

target-address	IPv4, IPv6, or Domain Name Server (DNS) target address to which the status of the gateway resources are reported. The format of the target address can be one of the following: • **ipv4:***ipv4-address* • **ipv6:***ipv6-address* • **dns:***domain-name*
resource-group	Maps the target address with the resource group index.
group-index	Resource group index. The range is from 1 to 5.
transport	(Optional) Specifies the mechanism to transport the RAI information.
tcp	(Optional) Transports the RAI information through Transmission Control Protocol (TCP).
tls	(Optional) Transports the RAI information through Transport Layer Security (TLS).
scheme	(Optional) Specifies the URL scheme for outgoing messages.
sip	(Optional) Selects SIP URL in outgoing OPTIONS message.
sips	(Optional) Selects Secure SIP (SIPS) URL in outgoing OPTIONS message.
udp	(Optional) Transports the RAI information through Unified Datagram Protocol (UDP).

Command Default

The SIP RAI mechanism is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **rai target** command to provide the details of SIP along with the index of the resource group that needs to be monitored for reporting over SIP trunk. A maximum of five RAI configurations can be applied for other destination targets or monitoring entities. However, only one RAI configuration is possible for one target address.

Examples

The following example shows how to enable reporting of SIP RAI information over TCP to a target address of example.com:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# rai target dns:example.com resource-group 1
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

random-contact

To populate an outgoing INVITE message with random-contact information (instead of clear-contact information), use the **random-contact** command in voice service VoIP SIP configuration mode. To disable random-contact information, use the **no** form of this command.

random-contact

no random-contact

Syntax Description

This command has no arguments or keywords.

Command Default

Outgoing INVITE messages are populated with clear-contact information.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

To populate outbound INVITE messages from the Cisco Unified Border Element with random-contact information instead of clear-contact information, use the **random-contact** command. This functionality will work only when the Cisco Unified Border Element is configured for Session Initiation Protocol (SIP) registration with random contact using the **credentials** and **registrar** commands.

Examples

The following example shows how to populate outbound INVITE messages with random-contact information:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# random-contact
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip random-contact	Populates the outgoing INVITE message with random-contact information at the dial-peer level.

random-request-uri validate

To enable the validation of the called number based on the random value generated during the registration of the number, use the **random-request-uri validate** command in voice service VoIP SIP configuration mode. To disable validation, use the **no** form of this command.

random-request-uri validate

no random-request-uri validate

Syntax Description

This command has no keywords or arguments.

Command Default

Validation is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The system generates a random string when registering a new number. An INVITE message with the P-Called-Party-ID value can have the Request-URI set to this random number. To enable the system to identify the called-number from the random number in the Request-URI, use the **random-request-uri validate** command.

If the P-Called-Party-ID is not set in the INVITE message, the Request URI for that message must contain the called party information (and cannot contain a random number). Therefore validation is performed only on INVITE messages with a P-Called-Party-ID.

Examples

The following example shows how to enable called-number validation at the global configuration level:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# random-request-uri validate
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.

Command	Description
register	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip random-request-uri validate	Validates the called number based on the random value generated during the registration of the number at the dial-peer configuration level.

ras retry

To configure the H.323 Registration, Admission, and Status (RAS) message retry counters, use the **ras retry** command in voice service h323 configuration mode. To set the counters to the default values, use the **no** form of this command.

ras retry {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value*

no ras retry {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**}

Syntax Description

all	Configures all RAS message counters that do not have explicit values configured individually. If **no ras retry all** is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message counter.
brq	Configures the bandwidth request (BRQ) message counter.
drq	Configures the disengage request (DRQ) message counter.
grq	Configures the gatekeeper request (GRQ) message counter.
rai	Configures the resource availability indication (RAI) message counter.
rrq	Configures the registration request (RRQ) message counter.
value	Number of times for the gateway to resend messages to the gatekeeper after the timeout period. The timeout period is the period in which a message has not been received by the gateway from the gatekeeper and is configured using the **ras timeout** command. Valid values are 1 through 30.

Command Default

arq: 2 retries
brq: 2 retries
drq: 9 retries
grq: 2 retries
rai: 9 retries
rrq: 2 retries

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras timeout** command. The **ras timeout** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and

gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the GRQ message counter set to 5 and all other RAS message counters set to 10:

```
Router(conf-serv-h323)# ras retry all 10
Router(conf-serv-h323)# ras retry grq 5
```

Related Commands

Command	Description
ras timeout	Configures the H.323 RAS message timeout values.

ras retry lrq

To configure the gatekeeper Registration, Admission, and Status (RAS) message retry counters, use the **ras retry lrq** command in gatekeeper configuration mode. To set the counters to the default values, use the **no** form of this command.

ras retry lrq *value*

no ras retry lrq

Syntax Description

lrq	Configures the location request (LRQ) message counter.
value	Number of times for the zone gatekeeper (ZGK) to resend messages to the directory gatekeeper (DGK) after the timeout period. The timeout period is the period in which a message has not been received by the ZKG from the DGK and is configured using the **ras timeout lrq** command. Valid values are 1 through 30.

Command Default

The retry counter is set to1.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras timeout lrq** command. The **ras timeout lrq** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry lrq** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the LRQ message counter set to 5:

```
Router(conf-gk)# ras retry lrq 5
```

Related Commands

Command	Description
ras timeout lrq	Configures the gatekeeper RAS message timeout values.

ras rrq dynamic prefixes

To enable advertisement of dynamic prefixes in additive registration request (RRQ) RAS messages on the gateway, use the **ras rrq dynamic prefixes** command in voice service h323 configuration mode. To disable advertisement of dynamic prefixes in additive RRQ messages, use the **no** form of this command.

ras rrq dynamic prefixes

no ras rrq dynamic prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.2(15)T, the default was set to enabled. In Cisco IOS Release 12.3(3), the default is set to disabled.

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(3)	The default is modified to be disabled by default.
12.3(4)T	The default change implemented in Cisco IOS Release 12.3(3) was integrated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

In Cisco IOS Release 12.2(15)T, the default for the **ras rrq dynamic prefixes** command was set to enabled so that the gateway automatically sent dynamic prefixes in additive RRQ messages to the gatekeeper. Beginning in Cisco IOS Release 12.3(3), the default is set to disabled, and you must specify the command to enable the functionality.

Examples

The following example allows the gateway to send advertisements of dynamic prefixes in additive RRQ messages to the gatekeeper:

```
Router(conf-serv-h323)# ras rrq dynamic prefixes
```

Related Commands

Command	Description
rrq dynamic-prefixes-accept	Enables processing of additive RRQ messages and dynamic prefixes on the gatekeeper.

ras rrq ttl

To configure the H.323 Registration, Admission, and Status (RAS) registration request (RRQ) time-to-live value, use the **ras rrq ttl** command in voice service h323 configuration mode. To set the RAS RRQ time-to-live value to the default value, use the **no** form of this command.

ras rrq ttl *time-to-live seconds* [**margin** *seconds*]

no ras rrq ttl

Syntax Description

time-to-live seconds	Number of seconds that the gatekeeper should consider the gateway active. Valid values are 15 through 4000. The *time-to-live seconds* value must be greater than the **margin** *seconds* value.
margin *seconds*	(Optional) The number of seconds that an RRQ message can be transmitted from the gateway before the time-to-live seconds value advertised to the gatekeeper. Valid values are 1 through 60. The **margin** *seconds* value times two must be less than or equal to the *time-to-live seconds* value.

Command Default

time-to-live seconds: 60 seconds
margin *seconds*: 15 seconds

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(6)	The maximum *time-to-live* value was changed from 300 to 4000 seconds.
12.3(4)T2	The maximum *time-to-live* value was changed from 300 to 4000 seconds.
12.3(7)T	The maximum *time-to-live* value was changed from 300 to 4000 seconds.

Usage Guidelines

Use this command to configure the number of seconds that the gateway should be considered active by the gatekeeper. The gateway transmits this value in the RRQ message to the gatekeeper. The **margin** *time* keyword and argument allow the gateway to transmit an early RRQ to the gatekeeper before the time-to-live value advertised to the gatekeeper.

Examples

The following example shows the *time-to-live seconds* value configured to 300 seconds and the **margin** *seconds* value configured to 60 seconds:

```
Router(conf-serv-h323)# ras rrq ttl 300 margin 60
```

ras timeout

To configure the H.323 Registration, Admission, and Status (RAS) message timeout values, use the **ras timeout** command in voice service h323 configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *seconds*

no ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**}

Syntax Description

all	Configures message timeout values for all RAS messages that do not have explicit values configured individually. If **no ras timeout all** is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message timer.
brq	Configures the bandwidth request (BRQ) message timer.
drq	Configures the disengage request (DRQ) message timer.
grq	Configures the gatekeeper request (GRQ) message timer.
rai	Configures the resource availability indication (RAI) message timer.
rrq	Configures the registration request (RRQ) message timer.
seconds	Number of seconds for the gateway to wait for a message from the gatekeeper before timing out. Valid values are 1 through 45.

Command Default

arq: 3 seconds
brq: 3 seconds
drq: 3 seconds
grq: 5 seconds
rai: 3 seconds
rrq: 5 seconds

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras retry** command. The **ras timeout** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the GRQ message timeout value set to 10 seconds and all other RAS message timeout values set to 7 seconds:

```
Router(conf-serv-h323)# ras timeout grq 10
Router(conf-serv-h323)# ras timeout all 7
```

Related Commands

Command	Description
ras retry	Configures the H.323 RAS message retry counters.

ras timeout decisec

To configure the H.323 Registration, Admission, and Status (RAS) message timeout values in deciseconds, use the **ras timeout decisec** command in voice service h323 configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} **decisec** *decisecond*

no ras timeout {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} **decisec**

Syntax Description

all	Configures message timeout values for all RAS messages that do not have explicit values configured individually. If **no ras timeout all** is entered, all values are set to the default except for the individual values that were configured separately.
arq	Configures the admission request (ARQ) message timer. Default: 3.
brq	Configures the bandwidth request (BRQ) message timer. Default: 3.
drq	Configures the disengage request (DRQ) message timer.Default: 3.
grq	Configures the gatekeeper request (GRQ) message timer. Default: 5.
rai	Configures the resource availability indication (RAI) message timer. Default: 3.
rrq	Configures the registration request (RRQ) message timer. Default: 5.
decisecond	Number of deciseconds for the gateway to wait for a message from the gatekeeper before timing out. Valid values are 1 through 45.

Command Default

Timers are set to their default values.

Command Modes

Voice service h323 configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **ras retry** command. The **ras timeout decisec** command configures the number of deciseconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples

The following example shows the ARQ message timeout value set to 25 deciseconds and all other RAS message timeout values set to 30 deciseconds:

```
Router(conf-serv-h323)# ras timeout arq decisec 25
Router(conf-serv-h323)# ras timeout all decisec 30
```

Related Commands

Command	Description
ras retry	Configures the H.323 RAS message retry counters.
ras timeout	Configures the H.323 RAS message timeout values in seconds.

ras timeout lrq

To configure the Gatekeeper Registration, Admission, and Status (RAS) message timeout values, use the **ras timeout lrq** command in gatekeeper configuration mode. To set the timers to the default values, use the **no** form of this command.

ras timeout lrq *seconds*

no ras timeout lrq

Syntax Description

lrq	Configures the location request (LRQ) message timer.
seconds	Number of seconds for the zone gatekeeper (ZGK) to wait for a message from the directory gatekeeper (DGK) before timing out. Valid values are 1 through 45. The default is 2.

Command Default Timers are set to their default value

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines Use this command in conjunction with the **ras retry lrq** command. The **ras timeout lrq** command configures the number of seconds for the zone gatekeeper (ZGK) to wait before resending a RAS message to a directory gatekeeper (DGK). The **ras retry lrq** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gatekeepers. For example, if you have gatekeepers that are slow to respond to a LRQ RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

Examples The following example shows the LRQ message timeout value set to 4 seconds:

```
Router(conf-gk)# ras timeout lrq 4
```

Related Commands

Command	Description
ras retry lrq	Configures the gatekeeper RAS message retry counters.

rbs-zero

To enable 1AESS switch support for T1 lines on the primary serial interface of an access server, use the **rbs-zero** command in serial interface configuration mode. To disable IAESS switch support, use the **no** form of this command.

rbs-zero [**nfas-int** *nfas-int-range*]

no rbs-zero [**nfas-int** *nfas-int-range*]

Syntax Description

nfas-int *nfas-int-range*	(Optional) Non-Facility Associated Signaling (NFAS) interface number. Range is from 0 to 32.

Command Default

1AESS switch support is disabled.

Command Modes

Serial interface configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command supports the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

Use this command to configure the primary serial interface of an access server connected to T1 lines to support 1AESS switches for dial-in and dial-out calls. Modem calls of 56K or a lower rate are accepted; 64K calls are rejected.

In IAESS mode, the following occurs:

- Modem calls are accepted and digital calls are rejected.
- The ABCD bit of the 8 bits in the incoming calls is ignored. The ABCD bit of the 8 bits in the outgoing modem calls is set to 0.

In non-1AESS mode, modem and digital calls are accepted.

Examples

The following example enables 1AESS switching support on T1 channel 0:

```
Router(config)# controller t1 1/0
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

```
Router(config)# interface serial 1/0:23
Router(config-if)# no ip address
Router(config-if)# isdn switch-type primary-ni
Router(config-if)# rbs-zero nfas-int 0
```

Related Commands

Command	Description
interface serial	Enters serial interface configuration mode.
isdn switch-type	Sets the switch type.
pri-group timeslots	Configures the PRI trunk for a designated operation.
show controllers t1	Displays information about the T1 links and the hardware and software driver information for the T1 controller.
show isdn nfas group	Displays all the members of a specified NFAS group or all NFAS groups.

reason-header override

To enable cause code passing from one SIP leg to another, use the **reason-header override** command in SIP UA configuration mode. To disable reason-header override, use the **no** form of this command.

reason-header override

no reason-header override

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(9)T	Usage guidelines were updated to include configuration requirements for SIP-to-SIP configurations.

Usage Guidelines

In an SIP-to-SIP configuration the **reason-header override** command must be configured to ensure cause code passing from the incoming SIP leg to the outgoing SIP leg.

Examples

The following example, shows the SIP user agent with reason-header override being configured.

```
Router(config)# sip-ua
Router(config-sip-ua)# reason-header override
```

Related Commands

Command	Description
sip-ua	Enables SIP UA configuration commands.

redial

To define speed-dial code for a Feature Speed-dial (FSD) to redial the last number dialed, use the **redial** command in STC application feature speed-dial configuration mode. To return the code to its default, use the **no** form of this command.

redial *keypad-character*

no redial

Syntax Description

keypad-character	Character string that can be dialed on a telephone keypad (0-9, *, #). Default: #. Before Cisco IOS Release 12.4(20)YA, this is a single character. In Cisco IOS Release 12.5(20)YA and later releases, the string can be any of the following: • A single character (0-9, *, #) • Two digits (00-99) • Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) In Cisco IOS Release 15.0(1)M and later releases, the string can also be any of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

The default value is # (number sign).

Command Modes

STC application feature speed-dial configuration (config-stcapp-fsd)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(20)YA	The length of the *keypad-character* argument was changed to 1 to 4 characters.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)M	This command was modified.

Usage Guidelines

This command changes the value of the speed-dial code for Redial from the default (#) to the specified value.

In Cisco IOS Release 12.4(20)YA and later releases, if the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this speed dial. Typically, phone users dial a Feature Speed-dial (FSD) consisting of a prefix plus a speed-dial code, for example *#. If the feature code is 78#, the phone user dials only 78#, without the FSD prefix, to access the corresponding feature.

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that is already being used for a feature access code (FAC) or another FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

In Cisco IOS Release 12.4(20)YA and later releases, if you attempt to configure this command with a value that precludes or is precluded by a feature code for a FAC or another FSD, you receive a message. If you configure this command with a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable access to that feature.

To display a list of all FACs and FSDs, use the **show stcapp feature codes** command.

Examples

The following example shows how to change the value of the speed-dial code for Redial from the default (#). In this configuration, a phone user must press ** on the keypad to redial the number that was most recently dialed on this line, regardless of what value is configured for the FSD prefix.

```
Router(config)# stcapp feature speed-dial
Router(config-stcapp-fsd)# redial **
Router(config-stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for feature speed-dial codes (FSDs).
prefix (stcapp-fsd)	Defines the prefix for feature speed-dials (FSDs).
show stcapp feature codes	Displays all feature access codes (FACs) and feature access codes (FSDs) that are available for the STC application.
speed dial	Designates a range of speed-dial codes for the STC application.
stcapp feature speed-dial	Enables feature speed-dials (FSDs) in STC application and enters STC application feature speed-dial configuration mode for changing values of the prefix and speed-dial codes from the default.

redirect contact order

To set the order of contacts in the 300 Multiple Choice message, use the **redirect contact order** command in SIP configuration mode. To reset the order of contacts to the default, use the **no** form of this command.

redirect contact order [**best-match** | **longest-match**]

no redirect contact order

Syntax Description

best-match	(Optional) Uses the current system configuration.
longest-match	(Optional) Uses the destination pattern longest match first, and then the second longest match, the third longest match, and so on. This is the default.

Command Default longest-match

Command Modes SIP configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines This command applies when a 300 Multiple Choice message is sent by a SIP gateway indicating that a call has been redirected and that there are multiple routes to the destination.

Enter SIP configuration mode after entering voice service VoIP configuration mode as shown in the following example.

Examples The following example uses the current system configuration to set the order of contact:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# redirect contact order best-match
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.

redirect ip2ip (dial peer)

To redirect SIP phone calls to SIP phone calls on a specific VoIP dial peer using the Cisco IOS Voice Gateway, use the **redirect ip2ip** command in dial peer configuration mode. To disable redirection, use the **no** form of this command.

redirect ip2ip

no redirect ip2ip

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection is disabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **redirect ip2ip** command must be configured on the inbound dial peer of the gateway. This command enables, on a per dial peer basis, IP-to-IP call redirection for the gateway.

To enable global IP-to-IP call redirection for all VoIP dial peers, use voice service configuration mode. To specify IP-to-IP call redirection for a specific VoIP dial peer, configure the dial peer in dial peer configuration mode.

Note When IP-to-IP redirection is configured in dial peer configuration mode, the configuration for the specific dial peer is activated only if the dial peer is an inbound dial peer. To enable IP-to-IP redirection globally, use **redirect ip2ip** (voice service) command.

Examples

The following example specifies that on VoIP dial peer 99, IP-to-IP redirection is set:

```
dial-peer voice 99 voip
 redirect ip2ip
```

Related Commands

Command	Description
redirect ip2ip (voice service)	Redirects SIP phone calls to SIP phone calls globally on a gateway using the Cisco IOS voice gateway.

redirect ip2ip (voice service)

To redirect SIP phone calls to SIP phone calls globally on a gateway using the Cisco IOS Voice Gateway, use the **redirect ip2ip** command in voice service configuration mode. To disable redirection, use the **no** form of this command.

redirect ip2ip

no redirect ip2ip

Syntax Description This command has no arguments or keywords.

Command Default Redirection is disabled.

Command Modes Voice service configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines Use this command to enable IP-to-IP call redirection globally on a gateway. Use the **redirect ip2ip** (dial peer) command to configure IP-to-IP redirection on a specific inbound dial peer.

Examples The following example specifies that all VoIP dial peers use IP-to-IP redirection:

```
voice service voip
 redirect ip2ip
```

Related Commands

Command	Description
redirect ip2ip (dial peer)	Redirects SIP phone calls to SIP phone calls on a specific VoIP dial peer using the Cisco IOS voice gateway.

redirection (SIP)

To enable the handling of 3*xx* redirect messages, use the **redirection** command in SIP UA configuration mode. To disable the handling of 3*xx* redirect messages, use the **no** form of this command.

redirection

no redirection

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection is enabled.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **redirection** command applies to all Session Initiation Protocol (SIP) VoIP dial peers configured on the gateway.

The default mode of SIP gateways is to process incoming 3*xx* redirect messages according to RFC 2543. However if redirect handling is disabled with the **no redirection** command, the gateway treats the incoming 3*xx* responses as 4*xx* error class responses. To reset the default processing of 3*xx* messages, use the **redirection** command.

Examples

The following example disables processing of incoming 3*xx* redirection messages:

```
Router(config)# sip-ua
Router(config-sip-ua)# no redirection
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.

refer-ood enable

To enable out-of-dialog refer (OOD-R) processing, use the **refer-ood enable** command in SIP user-agent configuration mode. To disable OOD-R, use the **no** form of this command.

refer-ood enable [*request-limit*]

no refer-ood enable

Syntax Description

request-limit	(Optional) Maximum number of concurrent incoming OOD-R requests that the router can process. Range: 1 to 500. Default: 500.

Command Default

OOD-R processing is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Out of dialog Refer allows applications to establish calls using the SIP gateway or Cisco Unified CME. The application sets up the call and the user does not dial out from their own phone.

Examples

The following example shows how to enable OOD-R:

```
Router(config)# sip-ua
Router(config-sip-ua)# refer-ood enable
```

Related Commands

Command	Description
authenticate (voice register global)	Defines the authenticate mode for SIP phones in a Cisco Unified CME or Cisco Unified SRST system.
credential load	Reloads a credential file into flash memory.
debug voip application	Displays all application debug messages.

register e164

To configure a gateway to register or deregister a fully-qualified dial-peer E.164 address with a gatekeeper, use the **register e164** command in dial peer configuration mode. To deregister the E.164 address, use the **no** form of this command.

register e164

no register e164

Syntax Description This command has no arguments or keywords.

Command Default No E.164 addresses are registered until you enter this command.

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400, and the Cisco AS5850 in this release.

Usage Guidelines Use this command to register the E.164 address of an analog telephone line attached to a foreign exchange station (FXS) port on a router. The gateway automatically registers fully qualified E.164 addresses. Use the **no register e164** command to deregister an address. Use the **register e164** command to register a deregistered address.

Before you automatically or manually register an E.164 address with a gatekeeper, you must create a dial peer (using the **dial-peer** command), assign an FXS port to the peer (using the **port** command), and assign an E.164 address using the **destination-pattern** command. The E.164 address must be a fully qualified address. For example, +5550112, 5550112, and 4085550112 are fully qualified addresses; 408555.... is not. E.164 addresses are registered only for active interfaces, which are those that are not shut down. If an FXS port or its interface is shut down, the corresponding E.164 address is deregistered.

Tip You can use the **show gateway** command to find out whether the gateway is connected to a gatekeeper and whether a fully qualified E.164 address is assigned to the gateway. Use the **zone-prefix** command to define prefix patterns on the gatekeeper, such as 408555...., that apply to one or more gateways.

Examples

The following command sequence places the gateway in dial peer configuration mode, assigns an E.164 address to the interface, and registers that address with the gatekeeper.

```
gateway1(config)# dial-peer voice 111 pots
gateway1(config-dial-peer)# port 1/0/0
gateway1(config-dial-peer)# destination-pattern 5550112
gateway1(config-dial-peer)# register e164
```

The following commands deregister an address with the gatekeeper.

```
gateway1(config)# dial-peer voice 111 pots
gateway1(config-dial-peer)# no register e164
```

The following example shows that you must have a connection to a gatekeeper and must define a unique E.164 address before you can register an address.

```
gateway1(config)# dial-peer voice 222 pots
gateway1(config-dial-peer)# port 1/0/0
gateway1(config-dial-peer)# destination 919555....
gateway1(config-dial-peer)# register e164
ERROR-register-e164:Dial-peer destination-pattern is not a full E.164 number
gateway1(config-dial-peer)# no gateway
gateway1(config-dial-peer)# dial-peer voice 111 pots
gateway1(config-dial-peer)# register e164
ERROR-register-e164:No gatekeeper
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
dial-peer (voice)	Enters dial peer configuration mode and specifies the method of voice encapsulation.
port (dial peer)	Associates a dial peer with a specific voice port.
show gateway	Displays the current gateway status.
zone prefix	Adds a prefix to the gatekeeper zone list.

registered-caller ring

To configure the Nariwake service registered caller ring cadence, use the **registered-caller ring** command in dial peer configuration mode.

registered-caller ring *cadence*

Syntax Description

cadence	A value of 0, 1, or 2. The default ring cadence for registered callers is 1 and for unregistered callers is 0. The on and off periods of ring 0 (normal ringing signals) and ring 1 (ringing signals for the Nariwake service) are defined in the NTT user manual.

Command Default

The default Nariwake service registered caller ring cadence is ring 1.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Usage Guidelines

If your ISDN line is provisioned for the I Number or dial-in services, you must also configure a dial peer by using the **destination-pattern not-provided** command. Either port 1 or port 2 can be configured under this dial peer. The router then forwards the incoming call to voice port 1. (See the "Examples" section below.

If more than one dial peer is configured with the **destination-pattern not-provided** command, the router uses the first configured dial peer for the incoming calls. To display the Nariwake ring cadence setting, use the **show run** command.

Examples

The following example sets the ring cadence for registered callers to 2.

```
pots country jp
dial-peer voice 1 pots
 registered-caller ring 2
```

Related Commands

Command	Description
destination-pattern not-provided	Specifies the port to receive the incoming calls that have no called-party number.

registrar

To enable Session Initiation Protocol (SIP) gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar, use the **registrar** command in SIP UA configuration mode. To disable registration of E.164 numbers, use the **no** form of this command.

registrar {**dhcp** | [*registrar-index*] *registrar-server-address* [**:***port*]} [**auth-realm** *realm*] [**expires** *seconds*] [**random-contact**] [**refresh-ratio** *ratio-percentage*] [**scheme** {**sip** | **sips**}] [**tcp**] [*type*] [**secondary**]

no registrar [*registrar-index* | **secondary**]

Syntax Description

dhcp	(Optional) Specifies that the domain name of the primary registrar server is retrieved from a DHCP server (cannot be used to configure secondary or multiple registrars).
registrar-index	(Optional) A specific registrar to be configured, allowing configuration of multiple registrars (maximum of six). Range is 1 to 6.
registrar-server-address	The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats: • **dns:***address*—the Domain Name System (DNS) address of the primary SIP registrar server (the **dns:** delimiter must be included as the first four characters). • **ipv4:***address*—the IP address of the SIP registrar server (the **ipv4:** delimiter must be included as the first five characters). • **ipv6:[***address*]—the IPv6 address of the SIP registrar server (the **ipv6:** delimiter must be included as the first five characters and the address itself must include opening and closing square brackets).
[**:***port*]	(Optional) The SIP port number (the colon delimiter is required).
auth-realm	(Optional) Specifies the realm for preloaded authorization.
realm	The realm name.
expires *seconds*	(Optional) Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600.
random-contact	(Optional) Specifies the Random String Contact header used to identify the registration session.
refresh-ratio *ratio-percentage*	(Optional) Specifies the registration refresh ratio, in percentage. Range is 1 to 100. Default is 80.
scheme {**sip**	**sips**}	(Optional) Specifies the URL scheme. The options are SIP (**sip**) or secure SIP (**sips**), depending on your software installation**.** The default is **sip**.
tcp	(Optional) Specifies TCP. If not specified, the default is User Datagram Protocol UDP.

type	(Optional) The registration type. **Note** The *type* argument cannot be used with the **dhcp** option.
secondary	(Optional) Specifies a secondary SIP registrar for redundancy if the primary registrar fails. This option is not valid if specifying DHCP or if configuring multiple registrars. **Note** You cannot configure any other optional settings once you enter the **secondary** keyword—specify all other settings first.

Command Default Registration is disabled.

Command Modes SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(6)T	This command was modified. The **tls** keyword and the **scheme** keyword with the *string* argument were added.
12.4(22)T	This command was modified. Support for IPv6 addresses was added.
12.4(22)YB	This command was modified. The **dhcp**, **random-contact and refresh-ratio** keywords were added. Additionally, the **aor-domain** keyword and the **tls** option for the **tcp** keyword were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. The *registrar-index* argument for support of multiple registrars on SIP trunks was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)T	This command was modified. The **auth-realm** keyword was added.

Usage Guidelines Use the **registrar dhcp** or **registrar** *registrar-server-address* command to enable the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars. In Cisco IOS Release 15.0(1)XA and later releases, endpoints on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco Unified Border Elements (Cisco UBEs), and Cisco Unified Communications Manager Express (Cisco Unified CME) can be registered to multiple registrars using the **registrar** *registrar-index* command.

By default, Cisco IOS SIP gateways do not generate SIP register messages.

Note When entering an IPv6 address, you must include square brackets around the address value.

Examples

The following example shows how to configure registration with a primary and secondary registrar:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.1 expires 14400 secondary
```

The following example shows how to configure a device to register with the SIP server address received from the DHCP server. The **dhcp** keyword is available only for configuration by the primary registrar and cannot be used if configuring multiple registrars.

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar dhcp expires 14400
```

The following example shows how to configure a primary registrar using an IP address with TCP:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.3 tcp
```

The following example shows how to configure a URL scheme with SIP security:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# retry invite 3
Router(config-sip-ua)# retry register 3
Router(config-sip-ua)# timers register 150
Router(config-sip-ua)# registrar ipv4:209.165.201.7 scheme sips
```

The following example shows how to configure a secondary registrar using an IPv6 address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar ipv6:[3FFE:501:FFFF:5:20F:F7FF:FE0B:2972] expires 14400
secondary
```

The following example shows how to configure all POTS endpoints to two registrars using DNS addresses:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 1 dns:example1.com expires 180
Router(config-sip-ua)# registrar 2 dns:example2.com expires 360
```

The following example shows how to configure the realm for preloaded authorization using the registrar server address:

```
Router> enable
Router# configure terminal
Router(config)# sip-ua
Router(config-sip-ua)# registrar 2 192.168.140.3:8080 auth-realm example.com expires 180
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
retry register	Sets the total number of SIP register messages to send.
show sip-ua register status	Displays the status of E.164 numbers that a SIP gateway has registered with an external primary or secondary SIP registrar.
timers register	Sets how long the SIP UA waits before sending register requests.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

registrar server

To enable the local Session Initiation Protocol (SIP) registrar, use the **registrar server** command in service SIP configuration mode. To disable the configuration, use the **no** form of this command.

registrar server [**expires** [**max** *value*] [**min** *value*]]

no registrar server

Syntax Description

expires	(Optional) Configures the registration expiry time.
max *value*	(Optional) Configures the maximum registration expiry time, in seconds. The range is from 120 to 86400. The default is 3600.
min *value*	(Optional) Configures the minimum registration expiry time, in seconds. The range is from 60 to 3600. The default is 60.

Command Default

The local SIP registrar is disabled.

Command Modes

Service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

You must enable the local SIP registrar by using the **registrar server** command before configuring the SIP registration on Cisco Unified Border Element (UBE).

Examples

The following example shows how to enable the local SIP registrar and set the maximum and minimum expiry values to 4000 and 100 seconds respectively:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# registrar server expires max 4000 min 100
```

Related Commands

Command	Description
registration passthrough	Configures SIP registration pass-through options at the global level.
voice-class sip registration passthrough	Configures SIP registration pass-through options on a dial peer.

registration retries

To set the number of times that Skinny Client Control Protocol (SCCP) tries to register with a Cisco Unified CallManager, use the **registration retries** command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

registration retries *retry-attempts*

no registration retries

Syntax Description

retry-attempts	Number of registration attempts. Range is 1 to 32. Default is 3.

Command Default

3 registration attempts

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to control the number of registration retries before SCCP confirms that it cannot register with the Cisco Unified CallManager. When SCCP confirms that it cannot register to the current Cisco Unified CallManager (if the number of registration requests sent without an Ack reaches the registration retries value), SCCP tries to register with the next Cisco Unified CallManager.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the registration retry attempts to meet your needs.

Examples

The following example sets the number of registration retries to 15:

```
Router(config-sccp-ccm)# registration retries 15
```

Related Commands

Command	Description
ccm group	Creates a Cisco Unified CallManger group and enters SCCP Cisco CallManager configuration mode.
registration timeout	Sets the length of time between registration messages sent from SCCP to the Cisco CallManager.

registration timeout

To set the length of time between registration messages sent from Skinny Client Control Protocol (SCCP) to the Cisco Unified CallManager, use the **registration timeout** command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the **no** form of this command.

registration timeout *seconds*

no registration timeout

Syntax Description

seconds	Time, in seconds, between registration messages. Range is 1 to 180. Default is 3.

Command Default

3 seconds

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Whenever SCCP sends the registration message to the Cisco Unified CallManager, it initiates this timer. Once the timeout occurs, it sends the next registration message unless the number of messages without an Ack reaches the number set by the **registration retries** command. Use this command to set the Cisco Unified CallManager registration timeout parameter value.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the registration timeout value to meet your needs.

Examples

The following example sets the length of time between registration messages sent from SCCP to the Cisco Unified CallManager to 12 seconds:

```
Router(config-sccp-ccm)# registration timeout 12
```

Related Commands

Command	Description
ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
registration retries	Sets the number of times that SCCP tries to register with the Cisco Unified CallManager.

registration passthrough

To configure the Session Initiation Protocol (SIP) registration pass-through options, use the **registration passthrough** command in service SIP configuration mode. To disable the configuration, use the **no** form of this command.

registration passthrough [**static**] [**rate-limit** [**expires** *value*] [**fail-count** *value*]] [**registrar-index** [*index*]]

no registration passthrough

Syntax Description

static	(Optional) Configures Cisco Unified Border Element (UBE) to use static registrar details for SIP registration. Cisco UBE works in point-to-point mode when the **static** keyword is used.
rate-limit	(Optional) Configures SIP registration pass-through rate limit options.
expires *value*	(Optional) Sets the expiry value for rate limiting, in seconds. The range is from 60 to 65535. The default value is 3600.
fail-count *value*	(Optional) Sets the fail count value for rate limiting. The range is from 2 to 20. The default value is 0.
registrar-index	(Optional) Configures the registrar index that is to be used for registration pass-through.
index	(Optional) Registration index value. The range is from 1 to 6.

Command Default

SIP registration pass-through options are not configured.

Command Modes

Service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

You can use the **registration passthrough** command to configure the following SIP pass-through functionalities:

- Back-to-back registration facility to register phones for call routing.
- Options to configure the rate-limiting values, such as the expiry time, fail-count, and a list of registrars to be used for registration.

Examples

The following example shows how to set the registrar index as 2 for the SIP registration pass-through rate-limiting:

```
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# registration passthrough static rate-limit registrar-index 2
```

Related Commands

Command	Description
voice-class sip registration passthrough static rate-limit	Sets the SIP registration pass-through rate limiting options on a dial peer.

rel1xx

To enable all Session Initiation Protocol (SIP) provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint, use the **rel1xx** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

rel1xx {**supported** *value* | **require** *value* | **disable**}

no rel1xx

Syntax Description

supported *value*	Supports reliable provisional responses. The *value* argument may have any value, as long as both the user-agent client (UAC) and user-agent server (UAS) configure it the same. This keyword, with *value* of 100rel, is the default.
require *value*	Requires reliable provisional responses. The *value* argument may have any value, as long as both the UAC and UAS configure it the same.
disable	Disables the use of reliable provisional responses.

Command Default

supported with the 100rel value

Command Modes

SIP configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

The use of resource reservation with SIP requires that the reliable provisional feature for SIP be enabled either at the VoIP dial-peer level or globally on the router.

There are two ways to configure reliable provisional responses:

- Dial peer configuration mode. You can configure reliable provisional responses for the specific dial peer only by using the **voice-class sip rel1xx** command.
- SIP configuration mode. You can configure reliable provisional responses globally by using the **rel1xx** command.

The **voice-class sip rel1xx** command in dial peer configuration mode takes precedence over the **rel1xx** command in global configuration mode with one exception: If the **voice-class sip rel1xx** command is used with the **system** keyword, the gateway uses what was configured under the **rel1xx** command in global configuration mode.

Enter SIP configuration mode from voice-service VoIP configuration mode as shown in the following example.

Examples

The following example shows use of the **rel1xx** command with the value 100rel:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# rel1xx supported 100rel
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip rel1xx	Provides provisional responses for calls on a dial peer basis.

remote-party-id

To enable translation of the SIP header Remote-Party-ID, use the **remote-party-id** command in SIP UA configuration mode. To disable Remote-Party-ID translation, use the **no** form of this command.

remote-party-id

no remote-party-id

Syntax Description

This command has no arguments or keywords.

Command Default

Remote-Party-ID translation is enabled

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

When the **remote-party-id** command is enabled, one of the following calling information treatments occurs:

- If a Remote-Party-ID header is present in the incoming INVITE message, the calling name and number extracted from the Remote-Party-ID header are sent as the calling name and number in the outgoing Setup message. This is the default behavior. Use the remote-party-id command to enable this option.
- When no Remote-Party-ID header is available, no translation occurs so the calling name and number are extracted from the From header and are sent as the calling name and number in the outgoing Setup message. This treatment also occurs when the feature is disabled.

Examples

The following example shows the Remote-Party-ID translation being enabled:

```
Router(config-sip-ua)# remote-party-id
```

Related Commands

Command	Description
debug ccsip events	Enables tracing of SIP SPI events.
debug ccsip messages	Enables SIP SPI message tracing.
debug isdn q931	Displays call setup and teardown of ISDN connections.
debug voice ccapi in out	Enables tracing the execution path through the call control API.

req-qos

To specify the desired quality of service to be used in reaching a specified dial peer, use the **req-qos** command in dial peer configuration mode. To restore the default value for this command, use the **no** form of this command.

req-qos {**best-effort | controlled-load | guaranteed-delay**} [{**audio bandwidth | video bandwidth**} **default | max** *bandwidth-value*]

no req-qos

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
controlled-load	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to assure that preferential service is received even when the bandwidth is overloaded.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.
audio bandwidth	(Optional) Specifies amount of bandwidth to be requested for audio streams.
default	Sets the default bandwidth to be requested for audio or video streams. • Audio streams—Range is 1 to 64 kbps; default value is 64 kbps. • Video streams—Range is 1 to 5000 kbps; default value is no maximum
max *bandwidth-value*	Sets the maximum bandwidth to be requested for audio streams. Range is 1 to 64 kbps; default value is no maximum.
video bandwidth	(Optional) Specifies the amount of bandwidth to be requested for video streams.
default *bandwidth-value*	Sets the default bandwidth to be requested for video streams. Range is 1 to 5000 kbps; default value is 384 kbps.
max *bandwidth-value*	(Optional) Sets the maximum bandwidth to be requested for video streams. .

Defaults

best-effort

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.3(4)T	Keywords added to support audio and video streams.

Usage Guidelines

Use the **req-qos** command to request a specific quality of service to be used in reaching a dial peer. Like **acc-qos**, when you issue this command, the Cisco IOS software reserves a certain amount of bandwidth so that the selected quality of service can be provided. Cisco IOS software uses Resource Reservation Protocol (RSVP) to request quality of service guarantees from the network.

This command is applicable only to VoIP dial peers.

Examples

The following example configures guaranteed-delay as the requested quality of service to a dial peer:

```
dial-peer voice 10 voip
 req-qos guaranteed-delay
```

The following example configures guaranteed-delay and requests a default bandwidth level of 768 kbps for video streams:

```
dial-peer voice 20 voip
 req-qos guaranteed-delay video bandwidth default 768
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for any inbound and outbound call on a VoIP dial peer.

request

To use SIP profiles to add, copy, modify, or remove Session Initiation Protocol (SIP) or Session Description Protocol (SDP) header value in a SIP request message, use the **request** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

request *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

no request *method* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

Syntax Description

method	Type of message to be added, modified, or removed. It can be one of the following values: • **ack**—SIP acknowledgment message. • **any**—Any SIP message. • **bye**—SIP BYE message. • **cancel**—SIP CANCEL message. • **comet**—SIP COMET message. • **info**—SIP INFO message. • **invite**—The first SIP INVITE message. • **notify**—SIP NOTIFY message. • **options**—SIP OPTIONS message. • **prack**—SIP PRACK message. • **publish**—SIP PUBLISH message. • **refer**—SIP REFER message. • **register**—SIP REGISTER message. • **reinvite**—SIP REINVITE message. • **subscribe**—SIP SUBSCRIBE message. • **update**—SIP UPDATE message.
sdp-header	Specifies an SDP header.
sip-header	Specifies a SIP header.
header-name	SDP or SIP header name.
add	Adds a header.
copy	Copies a header.
modify	Modifies a header.
remove	Removes a header.
string	String to be added, copied, modified, or removed as a header. **Note** If you use the **copy** keyword, you must provide a matching pattern followed by the variable name for the *string* argument.

Command Default SIP profiles are not modified to add, copy, modify, or remove SIP or SDP header values.

Command Modes Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines If there are interoperability issues with Cisco UBE, the Cisco UBE will not work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, and therefore enable Cisco UBE to work with SIP signaling.

Use the **request** command to modify SIP profiles for a request message. You can add, copy, modify, or remove SIP or SDP header values in an outgoing SIP request message.

Examples The following example shows how to copy a SIP header value in a SIP request message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# request invite sip-header contact copy "(.*)" u01
```

Related Commands

Command	Description
response	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from a SIP response message.

request peer-header

To use SIP profiles to copy a peer header from an outgoing Session Initiation Protocol (SIP) request message, use the **request peer-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

request *method* **peer-header sip** {**sip-req-uri** | *header-name*} **copy** *pattern variable*

no request *method* **peer-header sip** {**sip-req-uri** | *header-name*} **copy** *pattern variable*

Syntax Description

method	Type of message to be copied. You can specify any of the following values: • **ack**—SIP acknowledgment message. • **any**—SIP message. • **bye**—SIP BYE message. • **cancel**—SIP CANCEL message. • **comet**—SIP COMET message. • **info**—SIP INFO message. • **invite**—First SIP INVITE message. • **notify**—Specifies SIP NOTIFY message. • **options**—SIP OPTIONS message. • **prack**—SIP PRACK message. • **publish**—SIP PUBLISH message. • **refer**—SIP REFER message. • **register**—SIP REGISTER message. • **reinvite**—SIP REINVITE message. • **subscribe**—SIP SUBSCRIBE message. • **update**—SIP UPDATE message.
sip	Specifies that the SIP header must be copied from the peer call leg.
sip-req-uri	Specifies the SIP request Uniform Resource Identifier (URI) to be copied from the peer call leg.
header-name	Header name from which the values must be copied.
copy	Copies a header.
pattern	Match pattern.
variable	Variable to which the pattern value must be copied. The range is from u01 to u99.

Command Default No SIP profiles are modified to copy a peer header in an outgoing SIP request message.

Command Modes Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines If there are interoperability issues with Cisco UBE, then the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, and therefore enable Cisco UBE to work with SIP signaling.

Configure the **request peer-header** command to use SIP profiles to copy a peer header from an outgoing SIP request message.

Examples The following example shows how to copy a peer header in an outgoing SIP request message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# request invite peer-header sip contact copy "(.*)" u01
```

Related Commands

Command	Description
response peer-header	Uses SIP profiles to copy a peer header from an outgoing SIP response message.

request (XML transport)

To set the XML transport mode request handling parameters, use the **request** command in XML transport configuration mode. To disable the XML transport request parameter setting, use the **no** form of this command

request {**outstanding** *number* | **timeout** *seconds*}

no request

Syntax Description

outstanding	Maximum number of outstanding requests.
number	The valid range for the number of outstanding requests is from 1 to 10. The default is 1.
timeout	Response timeout at the transport level.
seconds	Specifies the number of seconds a request is active before it times out. Valid rangeis from 0 to 60 seconds. The default value is 0 (no timeout).

Command Default

The default for **outstanding** is 1 and the default for **timeout** is 0 (no timeout).

Command Modes

XML transport configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command to set the request timeout. A value of 0 seconds specifies no timeout. This timeout applies to the request being processed and not outstanding requests as described below. The specified timeout limits the amount of time between the request being dequeued by the application and the completion of the processing of that request.

Use this command to specify the number of outstanding requests allowed per application for the specified transport mode. The outstanding requests are those requests that are queued at the application for processing but have not yet been processed.

Examples

The following example shows how to enter XML transport configuration mode, set the XML transport request timeout to 10 seconds, and exit XML transport configuration mode:

```
Router(config)# ixi transport http
Router(conf-xml-trans)# request timeout 10
```

Related Commands

Command	Description
ixi transport http	Enters XML transport configuration mode.
ixi application mib	Enters XML application configuration mode.
response size (XML transport)	Set the XML transport fragment size.

reset

To reset a set of digital signal processors (DSPs), use the **reset** command in global configuration mode.

reset *number*

Syntax Description		
	number	Number of DSPs to be reset. Range is from 0 to 30.

Command Default No default behavior or values.

Command Modes Global configuration

Command History		
	12.0(5)XE	This command was introduced on the Cisco 7200 series.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example displays the reset command configuration for DSP 1:

```
reset 1
01:24:54:%DSPRM-5-UPDOWN: DSP 1 in slot 1, changed state to up
```

reset timer expires

To globally configure Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE) to reset the expires timer upon receipt of a Session Initiation Protocol (SIP) 183 Session In Progress message, use the **reset timer expires** command in voice service SIP configuration mode. To globally disable resetting of the expires timer upon receipt of SIP 183 messages, use the **no** form of this command.

reset timer expires 183

no reset timer expires 183

Syntax Description

183	Specifies resetting of the expires timer upon receipt of SIP 183 Session In Progress messages.

Command Default

The expires timer is not reset after receipt of SIP 183 Session In Progress messages and a session or call that is not connected within the default expiration time (three minutes) is dropped.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

In some scenarios, early media cut-through calls (such as emergency calls) rely on SIP 183 with session description protocol (SDP) Session In Progress messages to keep the session or call alive until receiving a FINAL SIP 200 OK message, which indicates that the call is connected. In these scenarios, the call can time out and be dropped if it does not get connected within the default expiration time (three minutes).

Note The expires timer default is three minutes. However, you can configure the expiration time to a maximum of 30 minutes using the **timers expires** command in SIP user agent (UA) configuration mode.

To prevent early media cut-through calls from being dropped because they reach the expires timer limit, use the **reset timer expires** command in voice service SIP configuration mode to globally enable all dial peers on Cisco Unified CME, Cisco IOS voice gateways, or Cisco UBEs to reset the expires timer upon receipt of any SIP 183 message.

To configure the reset timer expiration setting for an individual dial peer, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode. To disable the expires timer reset on receipt of SIP 183 messages function, use the **no reset timer expires** command in voice service SIP configuration mode.

Examples

The following example shows how to globally configure all dial peers on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer each time a SIP 183 message is received:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# reset timer expires 183
```

Related Commands

Command	Description
timers expires	Specifies how long a SIP INVITE request remains valid before it times out if no appropriate response is received for keeping the session alive.
voice-class sip reset timer expires	Configures an individual dial peer on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer upon receipt of a SIP 183 message.

resource (voice)

To configure parameters for monitoring resources, use the **resource** command in voice-class configuration mode. To disable the configuration for monitoring resources, use the **no** form of this command.

resource {**cpu** {**1-min-avg** | **5-sec-avg**} | **ds0** | **dsp** | **mem** {**io-mem** | **proc-mem** | **total-mem**}} [**threshold high** *threshold-value* **low** *threshold-value*]

no resource {**cpu** | **ds0** | **dsp** | **mem**}

Syntax Description

cpu	Reports the CPU utilization information.
1-min-avg	Collects the CPU data for an average of one minute.
5-sec-avg	Collects the CPU data for an average of five seconds.
ds0	Reports utilization information for the DS0 port.
dsp	Reports utilization information for the digital signal processor (DSP) channel.
mem	Reports the memory utilization information.
io-mem	Reports the input/output memory utilization information.
proc-mem	Reports the process memory utilization information.
total-mem	Reports the complete memory utilization information.
threshold	Configures the high and low threshold values for the critical resources.
high	(Optional) Configures the resource high watermark value.
low	(Optional) Configures the resource low watermark value.
threshold-value	Threshold value, in percentage.

Command Default

Critical gateway resources are not monitored.

Command Modes

Voice-class configuration mode (config-class)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **resource** command to configure parameters for critical resources such as CPU, memory, DS0, and DSP to report the utilization status to external entities using the gateway resources for call handling. You can use the **voice class resource-group** command to enter voice-class configuration mode and configure resource groups. Each resource group has a unique number that identifies a group of resources to be monitored.

When you configure the high watermark values for any of the monitoring resources, be sure not to use more resources than available on the gateway. The high and low watermark values for threshold only indicate that the gateway might run out of resources soon. However, the gateway must still be able to trigger threshold-based reporting to the routing/monitoring entity.

When you configure the low watermark value for the threshold, be sure not to underutilize the gateway resources.

Examples

The following example shows how to configure CPU to report the utilization information to the external entities:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 1
Router(config-class)# resource cpu 1-min-avg threshold high 10 low 2
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
rai target	Configures the SIP RAI mechanism.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

resource threshold

To configure a gateway to report H.323 resource availability to its gatekeeper, use the **resource threshold** command in gateway configuration mode. To disable gateway resource-level reporting, use the **no** form of this command.

resource threshold [**all**] [**high** *percentage-value*] [**low** *percentage-value*]

no resource threshold

Syntax Description

all	(Optional) High- and low-parameter settings are applied to all monitored H.323 resources. This is the default condition.
high *percentage-value*	(Optional) Resource utilization level that triggers a Resource Availability Indicator (RAI) message that indicates that H.323 resource use is high. Enter a number between 1 and 100 that represents the high-resource utilization percentage. A value of 100 specifies high-resource usage when any H.323 resource is unavailable. Default is 90 percent.
low *percentage-value*	(Optional) Resource utilization level that triggers an RAI message that indicates H.323 resource usage has dropped below the high-usage level. Enter a number between 1 and 100 that represents the acceptable resource utilization percentage. After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the **low** parameter. Default is 90 percent.

Command Default

Reports low resources when 90 percent of resources are in use and reports resource availability when resource use drops below 90 percent.

Command Modes

Gateway configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release

Usage Guidelines

This command defines the resource load levels that trigger RAI messages. To view the monitored resources, enter the **show gateway** command.

The monitored H.323 resources include digital signal processor (DSP) channels and DS0s. Use the **show call resource voice stats** command to see the total amount of resources available for H.323 calls.

Note The DS0 resources that are monitored for H.323 calls are limited to the ones that are associated with a voice POTS dial peer.

See the dial peer configuration commands for details on how to associate a dial peer with a PRI or channel-associated signaling (CAS) group.

When any monitored H.323 resources exceed the threshold level defined by the **high** parameter, the gateway sends an RAI message to the gatekeeper with the AlmostOutOfResources field flagged. This message reports high resource usage.

When all gateway H.323 resources drop below the level defined by the **low** parameter, the gateway sends the RAI message to the gatekeeper with the AlmostOutOfResources field cleared.

When a gatekeeper can choose between multiple gateways for call completion, the gatekeeper uses internal priority settings and gateway resource statistics to determine which gateway to use. When all other factors are equal, a gateway that has available resources is chosen over a gateway that has reported limited resources.

Examples

The following example defines the H.323 resource limits for a gateway.

```
gateway1(config-gateway)# resource threshold high 70 low 60
```

Related Commands

Command	Description
show call resource voice stats	Displays resource statistics for an H.323 gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.

resource-pool (mediacard)

To create a Digital Signal Processor (DSP) resource pool on ad-hoc conferencing and transcoding port adapters, use the **resource-pool** command in mediacard configuration mode. To remove the DSP resource pool and release the associated DSP resources, use the **no** form of this command.

resource-pool *identifier* **dsps** *number*

no resource-pool *identifier* **dsps** *number*

Syntax Description

identifier	Identifies the DSP resource to be configured. Valid values consist of alphanumeric characters, plus "_" and "-".
dsps	Digital signal processor.
number	Specifies the number of DSPs to be allocated for the specified resource pool. Valid values are from 1 to 4.

Command Default

No default behavior or values

Command Modes

Mediacard configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

The DSP resource pool identifier should be unique across the same Communication Media Module (CMM). Removing a resource pool may cause the profile using that resource pool to be disabled if it is the last resource pool in the profile.

Examples

The following example shows how to create a DSP resource pool:

```
resource-pool headquarters_location1 dsps 2
```

Related Commands

Command	Description
debug mediacard	Displays debugging information for DSPRM.
show mediacard	Displays information about the selected media card.

response

To use SIP profiles to add, copy, modify, or remove Session Initiation Protocol (SIP) or Session Description Protocol (SDP) header value in a SIP response message, use the **response** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

response *option* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

no response *option* {**sdp-header** | **sip-header**} *header-name* {**add** | **copy** | **modify** | **remove**} *string*

Syntax Description

option	Response code to be added, copied, modified, or removed. You can specify one of the following values: • *code*—Response code value. It can be one of the following values: – **100** – **180** to **183** – **200** – **102** – **300** to **302** – **305** – **380** – **400** to **423** – **480** to **489** – **491** – **493** – **500** to **505** – **515** – **580** – **600** – **603** – **604** – **606** • **any**—Adds, copies, modifies, or removes any response message.
sdp-header	Specifies SDP header.
sip-header	Specifies SIP header.
header-name	SDP or SIP header name.
add	Adds a header.
copy	Copies a header.
modify	Modifies a header.
remove	Removes a header.
string	String to be added as a header.

Command Default No SIP profile is modified to add, copy, modify, or remove a SIP header value.

Command Modes Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines If there are interoperability issues with Cisco UBE, the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP header values, to enable Cisco UBE to work with SIP signaling.

Use the **response** command to modify SIP profiles for a response message. You can add, copy, modify, or remove SIP or SDP header values in an outgoing SIP response message.

Examples The following example shows how to copy a SIP header value in a SIP response message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# response 409 sip-header to copy string1
```

Related Commands

Command	Description
request	Modifies a SIP profile to add, copy, modify, or remove a SIP or SDP header value from an outgoing SIP request message.

response (XML application)

To set XML application response parameters, use the **response** command in XML application configuration mode. To disable response parameter settings, use the **no** form of this command.

response {**formatted** | **timeout** {**-1** | *seconds*}}

no response {**formatted** | **timeout** {**-1** | *seconds*}}

Syntax Description

formatted	Response parameters in formatted human readable XML.
timeout	Application specified response timeout.
-1	Enter -1 to indicate no application specified timeout. This is the default timeout setting.
seconds	Number of seconds a response is active before it times out. Valid range includes 0 to 60 seconds.

Command Default

The default for the **timeout** keyword is **-1** indicating not application specified timeout.

Command Modes

XML application configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The response timeout specified in this command, if other than -1 which is the default, overwrites the timeout value specified in the request (XML transport) command that sets the timeout at the transport level.

The same http transport layer could have multiple applications active at the same time. You can set the timeout for each application individually or have all of the applications to use the same timeout value set at transport layer using the request (XML transport) command in XML transport configuration mode.

Examples

The following example shows how to enter XML application configuration mode, set XML response parameters in formatted human readable XML, and exit XML application configuration mode:

```
Router(config)# ixi application mib
Router(conf-xml-app)# response formatted
```

Related Commands

Command	Description
ixi application mib	Enters XML application configuration mode.
request (XML transport)	Set the XML transport mode request handling parameters.

response peer-header

To use SIP profiles to copy a peer header value in a SIP response message, use the **response peer-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

response {*code* | **any**} **peer-header sip** {**sip-req-uri** | *header-name*} **copy** *pattern variable*

no response *option* **peer-header sip** {**sip-req-uri** | *header-name*} **copy** *pattern variable*

Syntax Description

code	Response code to be copied. You can specify one of the following values: – **100** – **180** to **183** – **200** – **102** – **300** to **302** – **305** – **380** – **400** to **423** – **480** to **489** – **491** – **493** – **500** to **505** – **515** – **580** – **600** – **603** – **604** – **606** • **any**—Adds, copies, modifies, or removes any response message.
any	Adds, copies, modifies, or removes any response message.
sip	Specifies that the SIP header must be copied from the peer call leg.
sip-req-uri	Specifies the SIP request Uniform Resource Identifier (URI) to be copied from the peer call leg.
header-name	Header name from which the peer header values must be copied.
copy	Copies a header.
pattern	Match pattern.
variable	The destination variable name. The range is from u01 to u99.

Command Default No SIP profile is modified.

Command Modes Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines If there are interoperability issues with Cisco UBE, the Cisco UBE will not be able to work with the default SIP signaling. Hence, you must modify the SIP profiles to add, copy, modify, or remove SIP or SDP header values, to enable Cisco UBE to work with SIP signaling.

Use the **response peer-header** command to copy a peer header value in a SIP response message.

Examples The following example shows how to copy a peer header value in a SIP response message:

```
Router(config)# voice class sip-profiles 10
Router(config-class)# response 200 peer-header sip contact copy "(.*)" u01
```

Related Commands

Command	Description
request peer-header	Uses SIP profiles to copy a peer header value in a SIP request message.

response size (XML transport)

To set the response transport fragment size, use the **response size** command in XML transport configuration mode. To disable the response transport fragment size setting, use the **no** form of this command.

response size *kBps*

no response size

Syntax Description

kBps	Size of the fragment in the response buffer in kilobytes. Valid range is 1 to 64 kB. The default is 4 kB.

Command Modes

XML transport configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The fragment size is constrained by the transport type. The CLI help provides input guidelines.

Examples

The following example shows how to enter XML transport configuration mode, set XML transport fragment size to 32 Kbytes, and exit XML transport configuration mode:

```
Router(config)# ixi transport http
Router(conf-xml-trans)# response size 32
```

Related Commands

Command	Description
ixi transport http	Enters XML transport configuration mode.
ixi application mib	Enter XML application configuration mode.
request (XML transport)	Sets XML transport request handling parameters.

response-timeout

To configure the maximum time to wait for a response from a server, use the **response-timeout** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

response-timeout *seconds*

no **response-timeout** *seconds*

Syntax Description

seconds	Response waiting time, in seconds. Default is 1.

Command Default 1 second

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines If no response is received within the response-timeout time limit, the current connection ends, and the router attempts to contact the next service point.

Examples The following example sets response timeout to 1 second.

```
settlement 0
 response-timeout 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.
url	Specifies the Internet service provider address.

retries (auto-config application)

To set the number of download retry attempts for an auto-configuration application, use the **retries** command in auto-config application configuration mode. To reset to the default, use the **no** form of this command.

retries *number*

no retries

Syntax Description

number	Specifies the download retry attempts. Valid range is 1 to 3.

Command Default

The default value is 2.

Command Modes

Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **retries** command used to set the number of retries for an auto-configuration application to 3:

```
Router(auto-config-app)# retries 3
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
show auto-config	Displays the current status of auto-configuration applications.

retry bye

To configure the number of times that a BYE request is retransmitted to the other user agent, use the **retry bye** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry bye *number*

no retry bye *number*

Syntax Description

number	Number of BYE retries. Range is from 1 to 10. The default is 10.

Command Default 10 retries

Command Modes SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.

Usage Guidelines To reset this command to the default value, you can also use the **default** command.

Examples

```
The following example sets the number of BYE retries to 5.

sip-ua
 retry bye 5
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the SIP user-agent configuration commands, with which you configure the user agent.

retry cancel

To configure the number of times that a CANCEL request is retransmitted to the other user agent, use the **retry cancel** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry cancel *number*

no retry cancel *number*

Syntax Description

number	Number of CANCEL retries. Range is from 1 to 10. Default is 10.

Command Default 10 retries

Command Modes SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.

Usage Guidelines To reset this command to the default value, you can also use the **default** command.

Examples

```
The following example sets the number of cancel retries to 5.

sip-ua
 retry cancel 5
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the sip ua configuration commands, with which you configure the user agent.

retry comet

To configure the number of times that a COMET request is retransmitted to the other user agent, use the **retry comet** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry comet *number*

no retry comet

Syntax Description

number	Number of COMET retries. Range is from 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

COMET, or conditions met, indicates if preconditions for a given call or session have been met. This command is applicable only with calls (other than best-effort) that involve quality of service (QoS).

Use the default number of 10 retries, when possible. Lower values, such as 1, can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures a COMET request to be retransmitted 8 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry comet 8
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.

Command	Description
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry interval

To define the time between border element attempts delivery of unacknowledged call-detail-record (CDR) information, use the **retry interval** command in Annex G neighbor usage configuration mode. To reset to the default, use the **no** form of this command.

retry interval *seconds*

no retry interval

Syntax Description

seconds	Retry interval between delivery attempts, in seconds. Range is from 1 to 3600 (1 hour). The default is 900.

Command Default 900 seconds

Command Modes Annex G neighbor usage configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to set the interval during which the border element attempts delivery of unacknowledged call-detail-record (CDR) information.

Examples The following example sets the retry interval to 2700 seconds (45 minutes):

```
Router(config-nxg-neigh-usg)# retry interval 2700
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry window	Defines the total time for which a border element attempts delivery.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.
usage-indication	Enters the mode used to configure optional usage indicators.

retry invite

To configure the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent, use the **retry invite** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry invite *number*

no retry invite ***number***

Syntax Description

number	Number of INVITE retries. Range is from 1 to 10. Default is 6.

Command Default

6 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

When configuring SIP using SIP user-agent configuration commands such as the **retry invite** command, the use of the default values for the commands causes the rotary function to not take effect. The rotary function is when you set up more than one VoIP dial peer for the same destination pattern, and the dial peers are assigned to different targets. Assign different targets so that if the call cannot be set up with the first dial peer (preference one), the next dial peer can be tried.

To use the rotary function within SIP, set the retry value for the SIP **retry invite** command to 4 or less.

Examples

The following example sets the number of invite retries to 5.

```
sip-ua
 retry invite 5
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-ua	Enables the UA configuration commands, with which you configure the user agent.

retry keepalive (SIP)

To set the retry count for keepalive retransmission, use the **retry keepalive** command in SIP UA configuration mode. To restore the retry count to the default value for keepalive retransmission, use the **no** form of this command.

retry keepalive *count*

no retry keepalive *count*

Syntax Description

count	Retry keepalive retransmission value in the range from 1 to 10. The default value is 6.

Command Default

The default value for the retry keepalive retransmission is 6.

Command Modes

SIP UA configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Sets the keepalive retransmissions retry count.

Examples

The following example sets the retry for the keepalive retransmissions to 8:

```
sip-ua
 retry keepalive 8
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
keepalive trigger	Sets the trigger to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
timers keepalive	Sets the time interval between sending Options message requests when the SIP server is active or down.

retry notify

To configure the number of times that the notify message is retransmitted to the user agent that initiated the transfer or Refer request, use the **retry notify** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry notify *number*

no retry notify

Syntax Description

number	Number of notify message retries. Range is from 1 to 10. Default is 10.

Command Default 10 retries

Command Modes SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines A notify message informs the user agent that initiated the transfer or refer request of the outcome of the Session Initiation Protocol (SIP) transaction.

Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples The following example configures a notify message to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry notify 10
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
timers notify	Sets the amount of time that the user agent should wait before retransmitting the Notify message.

retry prack

To configure the number of times that the PRACK request is retransmitted to the other user agent, use the **retry prack** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry prack *number*

no retry prack

Syntax Description

number	Number of PRACK retries. Range is from 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

PRACK allows reliable exchanges of Session Initiation Protocol (SIP) provisional responses between SIP endpoints. Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures a PRACK request to be retransmitted 9 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry prack 9
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.

Command	Description
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry refer

To configure the number of times that the Refer request is retransmitted, use the **retry refer** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry refer *number*

no retry refer

Syntax Description

number	Number of Refer request retries. Range is from 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Usage Guidelines

A Session Initiation Protocol (SIP) Refer request is sent by the originating gateway to the receiving gateway and initiates call forward and call transfer capabilities.

When configuring the **retry refer** command, use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the receiving gateway.

Examples

The following example configures a Refer request to be retransmitted 10 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry refer 10
```

Related Commands

Command	Description
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry register

To set the total number of Session Initiation Protocol (SIP) register messages that the gateway should send, use the **retry register** command in SIP user-agent configuration mode. To reset this number to the default, use the **no** form of this command.

retry register *retries*

no retry register

Syntax Description

retries	Total number of register messages that the gateway should send. The range is from 1 to 10, and the default is 10 retries.

Command Default

The gateway sends ten retries.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the default number of 10 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example specifies that the gateway sends nine register messages:

```
sip-ua
 retry invite 9
 retry register 9
 timers register 150
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
timers register	Sets how long the SIP user agent waits before sending register requests.

retry rel1xx

To configure the number of times that the reliable 1*xx* response is retransmitted to the other user agent, use the **retry rel1xx** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry rel1xx *number*

no retry rel1xx

Syntax Description

number	Number of reliable 1*xx* retries. Range is from 1 to 10. Default is 6.

Command Default

6 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

Use the default number of 6 when possible. Lower values such as 1 can lead to an increased chance of the message not being received by the other user agent.

Examples

The following example configures the reliable 1*xx* response to be retransmitted 7 times:

```
Router(config)# sip-ua
Router(config-sip-ua)# retry rel1xx 7
```

Related Commands

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.

Command	Description
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
show sip-ua retry	Displays the SIP retry attempts.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.

retry response

To configure the number of times that the response message is retransmitted to the other user agent, use the **retry response** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

retry response *number*

no retry response

Syntax Description

number	Number of response retries. Range is from 1 to 10. Default is 6.

Command Default 6 retries

Command Modes SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines To reset this command to the default value, you can also use the **default** command.

Examples The following example sets the number of response retries to 5.

```
sip-ua
 retry response 5
```

Related Commands

Command	Description
default	Resets the value of a command to its default.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry rel1xx	Configures the number of times that the reliable 1*xx* response is retransmitted to the other user agent.
sip-ua	Enables the sip-ua configuration commands, with which you configure the user agent.

retry subscribe

To configure the number of times that a SIP SUBSCRIBE message is retransmitted to the other user agent, use the **retry subscribe** command in SIP UA configuration mode. To reset to the default, use the no form of this command.

retry subscribe *number*

no retry subscribe *number*

Syntax Description

number	Number of SUBSCRIBE retries. Range is 1 to 10. Default is 10.

Command Default

10 retries

Command Modes

SIP UA configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **retry timer** command to configure retry intervals for this command. The default value for **retry timer** is 1000 ms, and the range is 10 to 100. Setting the timer to lower values can cause the application to get a failure response more quickly.

Examples

The following example sets the number of subscribe retries to 5:

```
sip-ua
 retry subscribe 5
```

Related Commands

Command	Description
retry notify	Configures the number of times that the Notify message is resent to the user agent that initiated the Invite request.
retry timer	Configures the retry interval for resending SIP messages.
show sip-ua retry	Displays SIP user agent retry statistics.

retry window

To define the total time for which a border element attempts delivery, use the **retry window** command in Annex G neighbor usage configuration mode. To reset to the default, use the **no** form of this command.

retry window *window-value*

no retry window

Syntax Description

window-value	Window value, in minutes. Range is from 1 to 65535. Default is 1440 minutes (24 hours).

Command Default 1440 minutes (24 hours)

Command Modes Annex G neighbor usage configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to set the total time during which a border element attempts delivery of unacknowledged call-detail-record (CDR) information.

Examples The following example sets the retry window to 15 minutes:

```
Router(config-nxg-neigh-usg)# retry window 15
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.

Command	Description
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.
usage-indication	Enters the submode used to configure optional usage indicators.

retry-delay

To set the time between attempts to connect with the settlement provider, use the **retry-delay** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

retry-delay *seconds*

no retry-delay

Syntax Description

seconds	Interval, in seconds, between attempts to connect with the settlement provider. Range is from 1 to 600.

Command Default 2 seconds

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines After exhausting all service points for the provider, the router is delayed for the specified length of time before resuming connection attempts.

Examples The following example sets a retry value of 15 seconds:

```
settlement 0
 relay-delay 15
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.

retry-limit

To set the maximum number of attempts to connect to the provider, use the **retry-limit** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

retry-limit *number*

no retry-limit *number*

Syntax Description

number	Maximum number of connection attempts in addition to the first attempt. Default is 1.

Command Default 1 retry

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines If no connection is established after the configured number of retries has been attempted, the router ceases connection attempts. The retry limit number does not count the initial connection attempt. A retry limit of one (default) results in a total of two connection attempts to every service point.

Examples The following example sets the number of retries to 1:

```
settlement 0
 retry-limit 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after a communication exchange is complete.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.

Command	Description
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

ring

To set up a distinctive ring for your connected telephones, fax machines, or modems, use the **ring** command in interface configuration mode. To disable the ring, use the **no** form of this command.

ring *cadence-number*

no ring *cadence-number*

Syntax Description

cadence-number	Number that determines the ringing cadence. Range is from 0 to 2: • Type 0 is a primary ringing cadence—default ringing cadence for the country your router is in. • Type 1 is a distinctive ring—0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 0.4 seconds off. • Type 2 is a distinctive ring—0.4 seconds on, 0.2 seconds off, 0.4 seconds on, 0.2 seconds off, 0.8 seconds on, 4 seconds off.

Command Default 0

Command Modes Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines This command applies to Cisco 800 series routers.

You can specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, see to the *Cisco 800 Series Routers Software Configuration Guide*.

Examples The following example specifies the type 1 distinctive ring:

```
ring 1
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dial-peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call-waiting	Disables call waiting.

Command	Description
port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
pots distinctive-ring-guard-time	Specifies a delay during which a telephone port can be rung after a previous call is disconnected (for Cisco 800 series routers).
show dial-peer voice	Displays configuration information and call statistics for dial peers.

ring cadence

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

ring cadence {*pattern-number* | **define** *pulse interval*}

no ring cadence

To specify the ring pattern for external calls, use the **ring cadence external** command. It is supported only in STCAPP.

ring cadence external *patternXX* | **define**

To specify the ring cadence for internal calls, use the existing **ring cadence** command.

ring cadence *patternXX* | **define**

The syntax for the **ring cadence external** command is the same as for the **ring cadence** command.

Syntax Description

pattern-number	Predefined ring cadence patterns. Each pattern specifies a ring-pulse time and a ring-interval time. • **pattern01**—2 seconds on, 4 seconds off • **pattern02**—1 second on, 4 seconds off • **pattern03**—1.5 seconds on, 3.5 seconds off • **pattern04**—1 second on, 2 seconds off • **pattern05**—1 second on, 5 seconds off • **pattern06**—1 second on, 3 seconds off • **pattern07**—0.8 second on, 3.2 seconds off • **pattern08**—1.5 seconds on, 3 seconds off • **pattern09**—1.2 seconds on, 3.7 seconds off • **pattern09**—1.2 seconds on, 4.7 seconds off • **pattern11**—0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off • **pattern12**—0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off
define	User-definable ring cadence pattern. Each number pair specifies one ring-pulse time and one ring-interval time. You must enter numbers in pairs, and you can enter from 1 to 6 pairs. The second number in the last pair that you enter specifies the interval between rings.

pulse	Number (1 or 2 digits) specifying ring-pulse (on) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.
interval	Number (1 or 2 digits) specifying ring-interval (off) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

Command Default

Ring cadence defaults to the pattern that you specify with the **cptone** command.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series. The **patternXX** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
15.0(1)M	This command was modified. The **external** keyword was added to specify the ring pattern of external calls.

Usage Guidelines

The **patternXX** keyword provides preset ring cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence. On the Cisco 2600 and Cisco 3600 series routers, only one or two pairs of digits can be entered under the **define** keyword.

Examples

The following example sets the ring cadence to 1 second on and 2 seconds off on voice port 1/0/0:

```
voice-port 1/0/0
 ring cadence pattern04
```

Related Commands

Command	Description
cptone	Specifies the default tone, ring, and cadence settings according to country.
ring frequency	Specifies the ring frequency for a specified FXS voice port.

ring frequency

To specify the ring frequency for a specified Foreign Exchange Station (FXS) voice port, use the **ring frequency** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

ring frequency *hertz*

no ring frequency *hertz*

Syntax Description

hertz	Ring frequency, in hertz, used in the FXS interface. Valid entries are as follows: • Cisco 3600 series: 25 and 50. Default is 25.

Command Default

Cisco 3600 series routers: 25 Hz

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco MC3810.

Usage Guidelines

Use this command to select a specific ring frequency for an FXS voice port. Use the **no** form of this command to reset the default value. The ring frequency you select must match the connected equipment. If set incorrectly, the attached phone might not ring or might buzz. In addition, the ring frequency is usually country-dependent. You should take into account the appropriate ring frequency for your area before configuring this command.

This command does not affect ringback, which is the ringing a user hears when placing a remote call.

Examples

The following example sets the ring frequency on the voice port to 25 Hz:

```
voice-port 1/0/0
 ring frequency 25
```

Related Commands

Command	Description
ring cadence	Specifies the ring cadence for an FXS voice port.
ring number	Specifies the number of rings for a specified FXO voice port.

ring number

To specify the number of rings for a specified Foreign Exchange Office (FXO) voice port, use the **ring number** command in voice port configuration mode. To reset to the default, use the **no** form of this command.

ring number *number*

no ring number *number*

Syntax Description

number	Number of rings detected before answering the call. Range is from 1 to 10. The default is 1.

Command Default 1 ring

Command Modes Voice port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

Use this command to set the maximum number of rings to be detected before answering a call over an FXO voice port. Use the **no** form of this command to reset the default value, which is one ring.

Normally, this command should be set to the default so that incoming calls are answered quickly. If you have other equipment available on the line to answer incoming calls, you might want to set the value higher to give the equipment sufficient time to respond. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.

This command is not applicable to Foreign Exchange Station (FXS) or E&M interfaces because they do not receive ringing on incoming calls.

Examples

The following example sets 5 as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/0/0
 ring number 5
```

Related Commands

Command	Description
ring frequency	Specifies the ring frequency for a specified FXS voice port.

ringing-timeout

To define the timeout period for the SCCP telephony control (STC) application feature call back, use the **ringing-timeout** command in STC application feature callback configuration mode. To return to the default timeout period, use the **no** form of this command.

ringing-timeout *seconds*

no ringing-timeout

Syntax Description

seconds	Period of time in seconds. Range: 5 to 60. Default: 30.

Command Default

The default is 30 seconds.

Command Modes

STC application feature callback configuration (config-stcapp-callback)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command changes the timeout period of the ringing timer from the default of 30 seconds to the specified value.

The ringing timer specifies the number of seconds during which the calling device that is in a Callback on Busy condition can receive a Callback Ringing and after which, if the calling device does not answer, the CallBack on Busy condition is cancelled.

Examples

The following example shows how to change the timeout period of the ringing timer for CallBack on Busy from the default (30) to a new value (45).

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)# ringing-timer 45
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-code	Defines the callback activation key sequence for CallBack on Busy.

roaming (dial peer)

To enable roaming capability for a dial peer, use the **roaming** command in dial peer configuration mode. To disable roaming capability, use the **no** form of this command.

roaming

no roaming

Syntax Description This command has no arguments or keywords.

Command Default No roaming

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines Use this command to enable roaming capability of a dial peer if that dial peer can terminate roaming calls. If a dial peer is dedicated to local calls only, disable roaming capability.

The roaming dial peer must work with a roaming service provider. If the dial peer allows a roaming user to go through and the service provider is not roaming-enabled, the call fails.

Examples The following example enables roaming capability for a dial peer:

```
dial-peer voice 10 voip
roaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified *provider-number*.
settlement roam-pattern	Configures a pattern to match against when determining roaming.

roaming (settlement)

To enable roaming capability for a settlement provider, use the **roaming** command in settlement configuration mode. To disable roaming capability, use the **no** form of this command.

roaming

no roaming

Syntax Description This command has no arguments or keywords.

Command Default No roaming

Command Modes Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines Enable roaming capability of a settlement provider if that provider can authenticate a roaming user and route roaming calls.

A roaming call is successful only if both the settlement provider and the outbound dial peer for that call are roaming-enabled.

Examples The following example enables roaming capability for a settlement provider:

```
settlement 0
roaming
```

Related Commands

Command	Description
roaming (dial peer)	Enables the roaming capability for the dial peer.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified *provider-number*.
settlement roam-pattern	Configures a pattern to match against when determining roaming.

rrq dynamic-prefixes-accept

To enable processing of additive registration request (RRQ) RAS messages and dynamic prefixes on the gatekeeper, use the **rrq dynamic-prefixes-accept** command in gatekeeper configuration mode. To disable processing of additive RRQ messages and dynamic prefixes, use the **no** form of this command.

rrq dynamic-prefixes-accept

no rrq dynamic-prefixes-accept

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.2(15)T, the default was set to enabled. In Cisco IOS Release 12.3(3), the default is set to disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(3)	The default is modified to be disabled by default.
12.3(4)T	The default change implemented in Cisco IOS Release 12.3(3) was integrated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

In Cisco IOS Release 12.2(15)T, the default for the **rrq dynamic-prefixes-accept** command was set to enabled so that the gatekeeper automatically received dynamic prefixes in additive RRQ messages from the gateway. Beginning in Cisco IOS Release 12.3(3), the default is set to disabled, and you must specify the command to enable the functionality.

Examples

The following example allows the gatekeeper to process additive RRQ messages and dynamic prefixes from the gateway:

```
Router(config-gk)# rrq dynamic-prefixes-accept
```

Related Commands

Command	Description
ras rrq dynamic prefixes	Enables advertisement of dynamic prefixes in additive RRQ messages on the gateway.

rsvp

To enable RSVP support on a transcoding or MTP device, use the **rsvp** command in DSP farm profile configuration mode. To disable RSVP support, use the **no** form of this command.

rsvp

no rsvp

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes DSP farm profile configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines This command enables a transcoder or MTP device to register as RSVP-capable with Cisco Unified CallManager. The SCCP device acts as an RSVP agent under the control of Cisco Unified CallManager. To support RSVP, you must also enable the **codec pass-through** command.

Note This command is not supported in conferencing profiles.

Examples The following example enables RSVP support on the transcoding device defined by profile 200:

```
Router(config)# dspfarm profile 200 transcode
Router(config-dspfarm-profile)# rsvp
Router(config-dspfarm-profile)# codec pass-through
```

Related Commands

Command	Description
codec (DSP Farm profile)	Specifies the codecs supported by a DSP farm profile.
debug call rsvp-sync events	Displays events that occur during RSVP setup.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show sccp connections rsvp	Displays information about active SCCP connections that use RSVP.

rtcp keepalive

To configure RTP Control Protocol (RTCP) keepalive report generation and generate RTCP keepalive packets, use the **rtcp keepalive** command in voice service configuration mode. To disable the configuration, use the **no** form of this command.

rtcp keepalive

no rtcp keepalive

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled by default.

Command Modes

Voice service configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use this command to configure RTCP keepalive report generation and generate RTCP keepalive packets. The **no** form of the command restores the default behavior.

Examples

The following example shows how to configure RTCP keepalive report generation and generate RTCP keepalive packets:

```
Router> enable
Router# configure terminal
Router(config) voice service voip
Router(conf-voi-serv)# rtcp keepalive
```

Related Commands

Command	Description
debug voip rtcp	Enables debugging for RTCP packets.
debug voip rtp	Enables debugging for RTP packets.
debug ip rtp protocol	Enables debugging for RTP protocol.
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.

rtp payload-type

To identify the payload type of a Real-Time Transport Protocol (RTP) packet, use the **rtp payload-type** command in dial peer voice configuration mode. To remove the RTP payload type, use the **no** form of this command.

rtp payload-type {**cisco-cas-payload** *number* | **cisco-clear-channel** *number* | **cisco-codec-aacld** *number* | **cisco-codec-fax-ack** *number* | **cisco-codec-fax-ind** *number* | **cisco-codec-gsmamrnb** *number* | **cisco-codec-ilbc** *number* | **cisco-codec-isac** *number* | **cisco-codec-video-h263+** *number* | **cisco-codec-video-h264** *number* | **cisco-fax-relay** *number* | **cisco-pcm-switch-over-alaw** *number* | **cisco-pcm-switch-over-ulaw** *number* | **cisco-rtp-dtmf-relay** *number* | **lmr-tone** *number* | **nse** *number* | **nte** *number* | **nte-tone** *number*} [**comfort-noise** {**13** | **19**}]

no rtp payload-type {**cisco-cas-payload** *number* | **cisco-clear-channel** *number* | **cisco-codec-fax-ack** *number* | **cisco-codec-fax-ind** *number* | **cisco-codec-gsmamrnb** *number* | **cisco-codec-ilbc** *number* | **cisco-codec-video-h263+** *number* | **cisco-codec-video-h264** *number* | **cisco-fax-relay** *number* | **cisco-pcm-switch-over-alaw** *number* | **cisco-pcm-switch-over-ulaw** *number* | **cisco-rtp-dtmf-relay** *number* | **lmr-tone** *number* | **nse** *number* | **nte** *number* | **nte-tone** *number*} [**comfort-noise** {**13** | **19**}]

Syntax Description

cisco-cas-payload *number*	Cisco channel-associated signaling (CAS) RTP payload. Range: 96 to 127. Default: 123.
cisco-clear-channel *number*	Cisco clear-channel RTP payload. Range: 96 to 127. Default: 125.
cisco-codec-aacld *number*	Cisco MPEG-4 Advanced Audio Codec - Low Delay (AAC_LD) codec. Range: 96 to 127. Default: 114.
cisco-codec-fax-ack *number*	Cisco codec fax acknowledge. Range: 96 to 127. Default: 97.
cisco-codec-fax-ind *number*	Cisco codec fax indication. Range: 96 to 127. Default: 96.
cisco-codec-gsmamrnb *number*	Cisco Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec. Range: 96 to 127. Default: 117.
cisco-codec-ilbc *number*	Cisco internet Low Bitrate Codec (iLBC) codec. Range: 96 to 127. Default: 116.
cisco-codec-isac *number*	Cisco internet Speech Audio Codec (iSAC) codec. Range: 96 to 127. Default: 124.
cisco-codec-video-h263+ *number*	RTP video codec H.263+ payload type. Range: 96 to 127. Default: 118.
cisco-codec-video-h264 *number*	RTP video codec H.264 payload type. Range: 96 to 127. Default: 119.
cisco-fax-relay *number*	Cisco fax relay. Range: 96 to 127. Default: 122.
cisco-pcm-switch-over-alaw *number*	Cisco RTP pulse code modulation (PCM) codec switch over indication (a-law). Default: 8.
cisco-pcm-switch-over-ulaw *number*	Cisco RTP PCM codec switch over indication (mu-law). Default: 0.
cisco-rtp-dtmf-relay *number*	Cisco RTP dual-tone multifrequency (DTMF) relay. Range: 96 to 127. Default: 121.
lmr-tone *number*	LMR payload type. Range: 96 to 127. Default: 0. The default value is set by the **no rtp payload-type lmr-tone** command.

nse *number*	A named signaling event (NSE). Range: 96 to 117. Default: 100.
nte *number*	A named telephone event (NTE). Range: 96 to 127. Default: 101.
nte-tone *number*	RFC-2833 tone payload type. Range 96 to 127. Default: 101.
comfort-noise {**13** | **19**}	(Optional) RTP payload type of comfort noise. The July 2001 draft entitled *RTP Payload for Comfort Noise*, from the Internet Engineering Task Force (IETF) Audio/Video Transport (AVT) working group, designates 13 as the payload type for comfort noise. If you are connecting to a gateway that complies with the *RTP Payload for Comfort Noise* draft, use 13. Use 19 only if you are connecting to older Cisco gateways that use DSPware before version 3.4.32. **Note** This command option is not available on the Cisco AS5400 running NextPort digital signal processors (DSPs). This command option is available on the Cisco AS5400 only if the platform has a high-density packet voice/fax feature card (AS5X-FC) with one or more AS5X-PVDM2-64 DSP modules installed. This support was added in Cisco IOS Release 12.4(4)XC, and integrated into Release 12.4(9)T, and later 12.4T releases.

Command Default No RTP payload type is configured.

Command Modes Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(2)XB	This command was modified. The **nte** and **comfort-noise** keywords were added.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(4)XC	This command was modified. The **cisco-codec-gsmamrnb** keyword was added.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(11)T	This command was modified. The **cisco-codec-ilbc**, **cisco-codec-video-h263+**, and **cisco-codec-video-h264** keywords were added.
12.4(15)XY	This command was modified. The **lmr-tone** and **nte-tone** keywords were added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was modified. The **cisco-codec-isac** keyword was added.

Usage Guidelines

Use this command to identify the payload type of an RTP. Use this command after the **dtmf-relay** command is used to choose the NTE method of DTMF relay for a Session Initiation Protocol (SIP) call.

Configured payload types of NSE and NTE exclude certain values that have been previously hard-coded with Cisco-proprietary meanings. Do not use the following numbers, which have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 127.

Use of these values results in an error message when the command is entered. You must first reassign the value in use to a different unassigned number, for example:

```
rtp payload-type cisco-codec-ilbc 100
ERROR: value 100 in use!

rtp payload-type nse 105
rtp payload-type cisco-codec-ilbc 100
```

Examples

The following example shows how to identify the RTP payload type as GSMAMR-NB115:

```
Router(config-dial-peer)# rtp payload-type cisco-codec-gsmamrnb 115
```

The following example shows how to identify the RTP payload type as NTE 99:

```
Router(config-dial-peer)# rtp payload-type nte 99
```

The following example shows how to identify the RTP payload type for the iLBC as 100:

```
Router(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100
```

Related Commands

Command	Description
dtmf-relay	Specifies how an H.323 or SIP gateway relays DTMF tones between telephony interfaces and an IP network.

rtp send-recv

To configure a Cisco IOS Session Initiation Protocol (SIP) gateway to establish a bidirectional voice path as soon as it receives a SIP 183 PROGRESS message with Session Description Protocol (SDP), use the **rtp send-recv** command in voice service SIP configuration mode. To configure the gateway to establish a backward-only media cut-through voice path upon receipt of a 183 PROGRESS message with SDP that persists until the call progresses to the connect state, use the **no** form of this command.

rtp send-recv

no rtp send-recv

Syntax Description

This command has no arguments or keywords.

Command Default

A bidirectional voice path is established upon receipt of a 183 PROGRESS message with SDP.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The default behavior on a Cisco IOS SIP gateway is to establish a bidirectional voice path from the moment it receives a SIP 183 PROGRESS message with SDP. However, this can result in clipping on some voice platforms if both parties send audio at the same time, such as during a call setup process when interactive voice response (IVR) and a caller both speak simultaneously. To establish the voice path in the backward direction only until the call is connected, use the **no rtp send-recv** command in voice service SIP configuration mode.

A backward-only voice path operates only during the connection attempt—once a call is connected, the voice path automatically converts to bidirectional sending and receiving of Real-Time Transport Protocol (RTP) packets and RTP control packets (RTCPs). However, if the **no rtp send-recv** command is configured on a SIP gateway, no inband or RFC 2833-based dual tone multifrequency (DTMF) digits can be sent in the forward direction until after the call is connected and the bidirectional voice path is established.

Examples

The following example enables RTP backward-only media cut-through on a Cisco IOS SIP gateway:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# no rtp send-recv
```

rtp-ssrc multiplex

To multiplex Real-Time Transport Control Protocol (RTCP) packets with RTP packets and to send multiple synchronization source in RTP headers (SSRCs) in a RTP session, use the **rtp-ssrc multiplex** command in voice service or dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

Syntax Available Under Voice Service Configuration Mode

rtp-ssrc multiplex

no rtp-ssrc multiplex

Syntax Available Under Dial Peer Voice Configuration Mode

rtp-ssrc multiplex [**system**]

no rtp-ssrc multiplex [**system**]

Syntax Description

system	Uses the system value. This is the default value.

Command Default

Under voice service configuration mode, the **rtp-ssrc multiplex** command is not enabled and hence there is no interoperation with Cisco TelePresence System (CTS).

At the dial-peer level, the **rtp-ssrc multiplex** command uses the global configuration level settings.

Command Modes

Voice service configuration (conf-voi-serv)

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **rtc-ssrc multiplex** command is used for the interoperation with CTS.

Examples

The following example shows how to multiplex RTCP packets with RTP packets and send multiple SSRCs in a RTP session:

```
Router# configure terminal
Router(config)# dial-peer voice 234 voip
Router(config-dial-peer)# rtp-ssrc multiplex system
```

rtsp client session history duration

To specify how long to keep Real Time Streaming Protocol (RTSP) client history records in memory, use the **rtsp client session history duration** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client session history duration *minutes*

no rtsp client session history duration

Syntax Description

minutes	Duration, in minutes, to keep the record. Range is from 1 to 10000. Default is 10.

Command Default

10 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This release does not support any other Cisco platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example sets the duration for the RTSP session history to 500 minutes:

```
rtsp client session history duration 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
rtsp client session history records	Specifies the number of RTSP client session history records kept during the session.
show call application voice	Displays all TCL or MGCP scripts that are loaded.
show rtsp client session	Displays cumulative information about the RTSP session records.

rtsp client rtpsetup enable

To configure a router to send the IP address in a Real Time Streaming Protocol (RTSP) setup message, use the **rtsp client rtpsetup enable** command in global configuration mode. To disable the configuration, use the **no** form of this command.

rtsp client rtpsetup enable

no rtsp client rtpsetup enable

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples The following example shows how to configure a router to send the IP address in an RTSP setup message:

```
Router# configure terminal
Router(config)# rtsp client rtpsetup enable
```

Related Commands

Command	Description
rtsp client session history duration	Specifies how long to keep RTSP client history records in memory.
rtsp client timeout connect	Sets the number of seconds allowed for the router to establish a TCP connection to an RTSP server.

rtsp client session history records

To configure the number of records to keep in the Real Time Streaming Protocol (RTSP) client session history, use the **rtsp client session history records** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client session history records *number*

no rtsp client session history records ***number***

Syntax Description

number	Number of records to retain in a session history. Range is from 1 to 100000. Default is 50.

Command Default 50 records

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This release does not support any other Cisco platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples The following example specifies that a total of 500 records are to be kept in the RTSP client history:

```
rtsp client session history records 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an application that was loaded via the MGCP scripting package.
rtsp client session history duration	Specifies the how long the RTSP is kept during the session.
show call application voice	Displays all Tcl or MGCP scripts that are loaded.

rtsp client timeout connect

To set the number of seconds allowed for the router to establish a TCP connection to a Real -Time Streaming Protocol (RTSP) server, use the **rtsp client timeout connect** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client timeout connect *seconds*

no rtsp client timeout connect

Syntax Description

seconds	How long, in seconds, the router waits to connect to the server before timing out. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command determines when the router abandons its attempt to connect to an RTSP server and declares a timeout error, if a connection cannot be established after the specified number of seconds.

Examples

The following example sets the connection timeout to 10 seconds:

```
rtsp client timeout connect 10
```

Related Commands

Command	Description
rtsp client session history records	Sets the maximum number of records to store in the RTSP client session history.
rtsp client timeout message	Sets the number of seconds that the router waits for a response from an RTSP server.

rtsp client timeout message

To set the number of seconds that the router waits for a response from a Real -Time Streaming Protocol (RTSP) server, use the **rtsp client timeout message** command in global configuration mode. To reset to the default, use the **no** form of this command.

rtsp client timeout message *seconds*

no rtsp client timeout message

Syntax Description

seconds	How long, in seconds, the router waits for a response from the server after making a request. Range is 1 to 20.

Command Default 3 seconds

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines This command sets how long the router waits for the RTSP server to respond to a request before declaring a timeout error.

Examples The following example sets the request timeout to 10 seconds:

```
rtsp client timeout message 10
```

Related Commands

Command	Description
rtsp client session history records	Sets the maximum number of records to store in the RTSP client session history.
rtsp client timeout connect	Sets the number of seconds allowed for the router to establish a TCP connection to an RTSP server.

rule (ENUM configuration)

To define a rule for an ENUM match table, use the **rule** command in ENUM configuration mode. To delete the rule, use the **no** form of this command.

rule *rule-number preference /match-pattern/ /replacement-rule /domain-name*

no rule *rule-number preference /match-pattern/ /replacement-rule /domain-name*

Syntax Description

rule-number	Assigns an identification number to the rule. Range is from 1 to 2147483647.
preference	Assigns a preference value to the rule. Range is from 1 to 2147483647. Lower values have higher preference.
/match-pattern	Stream editor (SED) expression used to match incoming call information. The slash "/" is a delimiter in the pattern.
/replacement-rule	SED expression used to replace match-pattern in the call information. The slash "/" is a delimiter in the pattern.
/domain-name	Domain name to be used while the query to the DNS server is sent.

Command Default

No default behavior or values

Command Modes

ENUM configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Table 36 shows examples of match patterns, input strings, and result strings for the rule (voice translation-rule) command.

Table 36 Match Patterns, Input Strings and Result Strings

Match Pattern	Replacement Pattern	Input String	Result String	Description
`/^.*/`	`//`	`4085550100`	–	Any string to null string.
`/^456\(.*\)/`	`/555\1/`	`5550100`	`5550100`	Match from the beginning of the input string.
`/\(^...\)456\(...\)/`	`/\1555\2/`	`408555010`	`4085550100`	Match from the middle of the input string.
`/\(.*\)0100/`	`/\0199/`	`4085550100`	`4085550199`	Match from the end of the input string.

Table 36 Match Patterns, Input Strings and Result Strings (continued)

Match Pattern	Replacement Pattern	Input String	Result String	Description
/^1#\(.*\)/	/\1/	1#2345	2345	Replace match string with null string.
/^408...\(8333\)/	/555\1/	4085550100	5550100	Match multiple patterns.

Rules are entered in any order, but their preference number determines the sequence in which they are used for matching against the input string, which is a called number. A lower preference number is used before a higher preference number.

If a match is found, the input string is modified according to the replacement rule, and the E.164 domain name is attached to the modified number. This longer number is sent to a Domain Name System (DNS) server to determine a destination for the call. The server returns one or more URLs as possible destinations. The originating gateway tries to place the call using each URL in order of preference. If a call cannot be completed using any of the URLs, the call is disconnected.

Examples

The following example defines ENUM rule number 3 with preference 2. The beginning of the call string is checked for digits 9011; when a match is found, 9011 is replaced with 1408 and the call is sent out as an e164.arpa number.

```
Router(config)# voice enum-match-table number
 Router(config-enum)# rule 3 2 /^9011\(.*\)//+1408\1/ arpa
```

Related Commands

Command	Description
show voice enum-match-table	Displays the configuration of a voice ENUM match table.
test enum	Tests the ENUM rule.
voice enum-match-table	Initiates the definition of a voice ENUM match table.

rule (voice translation-rule)

To define a translation rule, use the **rule** command in voice translation-rule configuration mode. To delete the translation rule, use the **no** form of this command.

Match and Replace Rule

rule *precedence /match-pattern/ /replace-pattern/*
[**type** {*match-type replace-type*} [**plan** {*match-type replace-type*}]]

no rule *precedence*

Reject Rule

rule *precedence* **reject** */match-pattern/* [**type** *match-type* [**plan** *match-type*]]

no rule *precedence*

Syntax Description

precedence	Priority of the translation rule. Range is from 1 to 15.
/match-pattern/	Stream editor (SED) expression used to match incoming call information. The slash '/' is a delimiter in the pattern.
/replace-pattern/	SED expression used to replace the match pattern in the call information. The slash '/' is a delimiter in the pattern.
type *match-type replace-type*	(Optional) Number type of the call. Valid values for the *match-type* argument are as follows: • **abbreviated**—Abbreviated representation of the complete number as supported by this network. • **any**—Any type of called number. • **international**—Number called to reach a subscriber in another country. • **national**—Number called to reach a subscriber in the same country, but outside the local network. • **network**—Administrative or service number specific to the serving network. • **reserved**—Reserved for extension.**subscriber**—Number called to reach a subscriber in the same local network. • **unknown**—Number of a type that is unknown by the network. Valid values for the *replace-type* argument are as follows: • **abbreviated**—Abbreviated representation of the complete number as supported by this network. • **international**—Number called to reach a subscriber in another country. • **national**—Number called to reach a subscriber in the same country, but outside the local network.

type *match-type replace-type* (continued)	• **network**—Administrative or service number specific to the serving network. • **reserved**—Reserved for extension. • **subscriber**—Number called to reach a subscriber in the same local network. • **unknown**—Number of a type that is unknown by the network.
plan *match-type replace-type*	(Optional) Numbering plan of the call. Valid values for the *match-type* argument are as follows: • **any**—Any type of dialed number. • **data** • **ermes** • **isdn** • **national**—Number called to reach a subscriber in the same country, but outside the local network. • **private** • **reserved**—Reserved for extension. • **telex** • **unknown**—Number of a type that is unknown by the network. Valid values for the *replace-type* argument are as follows: • **data** • **ermes** • **isdn** • **national**—Number called to reach a subscriber in the same country, but outside the local network. • **private** • **reserved**—Reserved for extension. • **telex** • **unknown**—Number of a type that is unknown by the network.
reject	The match pattern of a translation rule is used for call-reject purposes.

Command Default No default behavior or values

Command Modes Voice translation-rule configuration

Command History

Release	Modification
12.2(11)T	This command was introduced with a new syntax in voice-translation-rule configuration mode.

Usage Guidelines

Note Use this command in conjunction after the **voice translation-rule** command. An earlier version of this command uses the same name but is used after the **translation-rule** command and has a slightly different command syntax. In the older version, you cannot use the square brackets when you are entering command syntax. They appear in the syntax only to indicate optional parameters, but are not accepted as delimiters in actual command entries. In the newer version, you can use the square brackets as delimiters. Going forward, we recommend that you use this newer version to define rules for call matching. Eventually, the **translation-rule** command will not be supported.

A translation rule applies to a calling party number (automatic number identification [ANI]) or a called party number (dialed number identification service [DNIS]) for incoming, outgoing, and redirected calls within Cisco H.323 voice-enabled gateways.

Number translation occurs several times during the call routing process. In both the originating and terminating gateways, the incoming call is translated before an inbound dial peer is matched, before an outbound dial peer is matched, and before a call request is set up. Your dial plan should account for these translation steps when translation rules are defined.

Table 37 shows examples of match patterns, input strings, and result strings for the rule (voice translation-rule) command.

Table 37 Match Patterns, Input Strings and Result Strings

Match Pattern	Replacement Pattern	Input String	Result String	Description
/^.*/	//	4085550100	–	Any string to null string.
//	//	4085550100	4085550100	Match any string but no replacement. Use this to manipulate the call plan or call type.
/\(^...\)456\(...\)/	/\1555\2/	4084560177	4085550177	Match from the middle of the input string.
/\(.*\)0120/	/\10155/	4081110120	4081110155	Match from the end of the input string.
/^1#\(.*\)/	/\1/	1#2345	2345	Replace match string with null string.
/^408...\(8333\)/	/555\1/	4087770100	5550100	Match multiple patterns.
/1234/	/00&00/	5550100	55500010000	Match the substring.
/1234/	/00\000/	5550100	55500010000	Match the substring (same as &).

The software verifies that a replacement pattern is in a valid E.164 format that can include the permitted special characters. If the format is not valid, the expression is treated as an unrecognized command.

The number type and calling plan are optional parameters for matching a call. If either parameter is defined, the call is checked against the match pattern and the selected type or plan value. If the call matches all the conditions, the call is accepted for additional processing, such as number translation.

Several rules may be grouped together into a translation rule, which gives a name to the rule set. A translation rule may contain up to 15 rules. All calls that refer to this translation rule are translated against this set of criteria.

The precedence value of each rule may be used in a different order than that in which they were typed into the set. Each rule's precedence value specifies the priority order in which the rules are to be used. For example, rule 3 may be entered before rule 1, but the software uses rule 1 before rule 3.

The software supports up to 128 translation rules. A translation profile collects and identifies a set of these translation rules for translating called, calling, and redirected numbers. A translation profile is referenced by trunk groups, source IP groups, voice ports, dial peers, and interfaces for handling call translation.

Examples

The following example applies a translation rule. If a called number starts with 5550105 or 70105, translation rule 21 uses the rule command to forward the number to 14085550105 instead.

```
Router(config)# voice translation-rule 21
 Router(cfg-translation-rule)# rule 1 /^5550105/ /14085550105/
 Router(cfg-translation-rule)# rule 2 /^70105/ /14085550105/
```

In the next example, if a called number is either 14085550105 or 014085550105, after the execution of translation rule 345, the forwarding digits are 50105. If the match type is configured and the type is not "unknown," dial-peer matching is required to match the input string numbering type.

```
Router(config)# voice translation-rule 345
 Router(cfg-translation-rule)# rule 1 /^14085550105/ /50105/ plan any national
 Router(cfg-translation-rule)# rule 2 /^014085550105/ /50105/ plan any national
```

Related Commands

Command	Description
show voice translation-rule	Displays the parameters of a translation rule.
voice translation-rule	Initiates the voice translation-rule definition.

Cisco IOS Voice Commands: S

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

sccp

To enable the Skinny Client Control Protocol (SCCP) protocol and its related applications (transcoding and conferencing), use the **sccp** command in global configuration mode. To disable the protocol, use the **no** form of this command.

sccp

no sccp

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

SCCP and its related applications (transcoding and conferencing) become enabled only if digital-signal-processor (DSP) resources for these applications are configured, DSP-farm service is enabled, and the Cisco CallManager registration process is completed.

The **no** form of this command disables SCCP and its applications by unregistering from the active Cisco CallManager, dropping existing connections, and freeing allocated resources.

Examples The following example sets related values and then enables SCCP:

```
Router(config)# sccp ccm 10.10.10.1 priority 1
Router(config)# sccp local fastEthernet 0/0
Router(config)# sccp switchback timeout guard 180
Router(config)# sccp ip precedence 5
Router(config)# sccp
Router(config)# end
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
show dspfarm	Displays summary information about DSP resources.
show sccp	Displays the SCCP configuration information and current status.

sccp blf-speed-dial retry-interval

To set the retry timeout for Busy Lamp Field (BLF) notification for speed-dial numbers on SCCP phones registered to an external Cisco Unified CME router, use the **sccp blf-speed-dial retry-interval** command in presence configuration mode. To reset to the default, use the **no** form of this command.

sccp blf-speed-dial retry-interval *seconds* **limit** *number*

no sccp blf-speed-dial retry-interval

Syntax Description

seconds	Retry timeout in seconds. Range: 60 to 3600. Default: 60.
limit *number*	Maximum number of retries. Range: 10 to 100. Default: 10.

Command Default

Retry timeout is 60 seconds; retry limit is 10.

Command Modes

Presence configuration (config-presence)

Command History

Cisco IOS Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command specifies how frequently the router attempts to subscribe for the line status of an external directory number when the BLF speed-dial feature is configured on a SCCP phone. This retry mechanism is used when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. If the subscribe request toward the external server fails after the configured number of retries, the subscribe request from the phone is rejected.

Examples

The following example shows the BLF speed-dial retry interval set to 100 seconds and the limit to 25:

```
Router(config)# presence
Router(config-presence)# sccp blf-speed-dial retry-interval 100 limit 25
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.

sccp ccm

To add a Cisco Unified Communications Manager server to the list of available servers and set various parameters—including IP address or Domain Name System (DNS) name, port number, and version number—use the **sccp ccm** command in global configuration mode. To remove a particular server from the list, use the **no** form of this command.

NM-HDV or NM-HDV-FARM Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **priority** *priority* [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

NM-HDV2 or NM-HD-1V/2V/2VE Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

Syntax Description

ipv4-address	IPv4 address of the Cisco Unified Communications Manager server.
ipv6-address	IPv6 address of the Cisco Unified Communications Manager server.
dns	DNS name.
identifier *identifier-number*	Specifies the number that identifies the Cisco Unified Communications Manager server. The range is 1 to 65535.
priority *priority*	Specifies the priority of this Cisco Unified Communications Manager server relative to other connected servers. The range is 1 (highest) to 4 (lowest). **Note** This keyword is required only for NM-HDV and NM-HDV-FARM modules. Do not use this keyword if you are using the NM-HDV2 or NM-HD-1V/2V/2VE; set the priority using the **associate ccm** command in the Cisco Unified Communications Manager group.
port *port-number*	(Optional) Specifies the TCP port number. The range is 1025 to 65535. The default is 2000.
version *version-number*	(Optional) Cisco Unified Communications Manager version. Valid versions are **3.0**, **3.1**, **3.2**, **3.3**, **4.0**, **4.1**, **5.0.1**, **6.0**, and **7.0+**. There is no default value.
trustpoint	(Optional) Specifies the trustpoint for Cisco Unified Communications Manager certificate.
label	Cisco Unified Communications Manager trustpoint label.

Command Default

The default port number is 2000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.3(8)T	This command was modified. The **identifier** keyword and additional values for Cisco Unified Communications Manager versions were added.
12.4(11)XW	This command was modified. The **6.0** keyword was added to the list of version values.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. Support for IPv6 was added. The **version** keyword and *version-number* argument were changed from being optional to being required, and the **7.0+** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **trustpoint** keyword and the *label* argument were added.

Usage Guidelines

You can configure up to four Cisco Unified Communications Manager servers—a primary and up to three backups—to support digital signal processor (DSP) farm services. To add the Cisco Unified Communications Manager server to a Cisco Unified Communications Manager group, use the **associate ccm** command.

IPv6 support is provided for registration with Cisco Unified CM version 7.0 and later.

To enable Ad Hoc or Meet-Me hardware conferencing in Cisco Unified CME, you must first set the **version** keyword to **4.0** or a later version.

Beginning with Cisco IOS Release 12.4(22)T users manually configuring the **sccp ccm** command must provide the version. Existing router configurations are not impacted because automatic upgrade and downgrade are supported.

Examples

The following example shows how to add the Cisco Unified Communications Manager server with IP address 10.0.0.0 to the list of available servers:

```
Router(config)# sccp ccm 10.0.0.0 identifier 3 port 1025 version 4.0
```

The following example shows how to add the Cisco Unified CallManager server whose IPv6 address is 2001:DB8:C18:1::102:

```
Router(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.

Command	Description
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.
show sccp	Displays SCCP configuration information and current status.

sccp ccm group

To create a Cisco Unified Communications Manager group and enter SCCP Cisco CallManager configuration mode, use the **sccp ccm group** command in global configuration mode. To remove a particular Cisco Unified Communications Manager group, use the **no** form of this command.

sccp ccm group *group-number*

no sccp ccm group *group-number*

Syntax Description

group-number	Number that identifies the Cisco Unified Communications Manager group. Range is 1 to 50.

Command Default

No groups are defined, so all servers are configured individually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The number of group number range was increased to 50.

Usage Guidelines

Use this command to group Cisco Unified Communications Manager servers that are defined using the **sccp ccm** command. You can associate designated DSP farm profiles using the **associate profile** command so that the DSP services are controlled by the Cisco Unified Communications Manager servers in the group.

Examples

The following example enters SCCP Cisco CallManager configuration mode and associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 10:

```
Router(config)# sccp ccm group 10
Router(config-sccp-ccm)# associate ccm 25 priority 2
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group.
bind interface	Binds an interface with a Cisco Unified Communications Manager group.

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers.

sccp codec mask

To mask a codec type so that it is not used by Cisco CallManager, use the **sccp codec mask** command in global configuration mode. To unmask a codec, use the **no** form of this command.

sccp codec *codec* **mask**

no sccp codec *codec* **mask**

Syntax Description

codec	Codec to mask. Values are the following: • **g711alaw** • **g711ulaw** • **g729abr8** • **g729ar8** • **g729br8** • **g729r8**

Command Default No codecs are masked.

Command Modes Global configuration

Command History

Release	Modification
12.1(5)YH4	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(11)XJ2	The **gsmefr** and **gsmfr** keywords were removed as configurable codec options for all platforms with the exception of the **gsmfr** codec on the Cisco AS5400 and AS5350 with MSAv6 dsps.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines This command prevents the voice gateway from reporting codec types that are masked so that Cisco CallManager only selects codec types that are supported by the endpoints.

Note You must enable this command before Skinny Client Control Protocol (SCCP) is enabled. If the **sccp codec mask** command is used when SCCP is active, you must disable the SCCP using the **no sccp** command and then re-enable **sccp** for the **sccp codec mask** command to take effect.

Examples

The following example shows how to mask codec type G.711 ulaw and G.729r8:

```
sccp codec g711ulaw mask
sccp codec g729r8 mask
```

Related Commands

Command	Description
sccp	Enables SCCP and related applications.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
sccp local	Selects the local interface that SCCP applications use to register with Cisco CallManager.
show sccp	Displays SCCP configuration information and current status.

sccp ip precedence

To set the IP precedence value to be used by Skinny Client Control Protocol (SCCP), use the **sccp ip precedence** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp ip precedence *value*

no sccp ip precedence

Syntax Description

value	IP precedence value. Range is from 1 (lowest) to 7 (highest).

Command Default 5

Command Modes Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

Examples The following example sets IP precedence to the highest possible value:

```
Router# sccp ip precedence 1
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp local

To select the local interface that Skinny Client Control Protocol (SCCP) applications (transcoding and conferencing) use to register with Cisco CallManager, use the **sccp local** command in global configuration mode. To deselect the interface, use the **no** form of this command.

sccp local *interface-type interface-number* [**port** *port-number*]

no sccp local *interface-type interface-number*

Syntax Description

interface-type	Interface type that the SCCP application uses to register with Cisco CallManager. The type can be an interface address or a virtual-interface address such as Ethernet.
interface-number	Interface number that the SCCP application uses to register with Cisco CallManager.
port *port-number*	(Optional) Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The **port** keyword and *port-number* argument were added.

Usage Guidelines

The router must be equipped with one or more voice network modules that provide DSP resources.

Note If the default port is used by another application, the SCCP application fails to register to Cisco CallManager. Use the **port** keyword with the *port-number* argument to specify a different port for SCCP to use for registering with Cisco CallManager.

Examples

The following example selects a Fast Ethernet interface for SCCP applications to use to register with Cisco CallManager:

```
sccp local FastEthernet 0/0
```

Related Commands

Command	Description
dsp services dspfarm	Enables DSP-farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp plar

To enter SCCP PLAR configuration mode, use the **sccp plar** command in global configuration mode. To disable private line automatic ringdown (PLAR) on all ports, use the **no** form of this command.

sccp plar

no sccp plar

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (PLAR is not enabled on any port).

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used for enabling PLAR features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Use the **voiceport** command to enable a specific analog voice port for PLAR.

Examples

The following example sets PLAR on voice ports 2/0, 2/1, and 2/3:

```
Router(config)# sccp plar
Router(config-sccp-plar)# voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
Router(config-sccp-plar)# voiceport 2/1 dial 3264 digit 678,,,9*0,,#123 interval 100
Router(config-sccp-plar)# voiceport 2/3 dial 3478 digit 34567 wait-connect 500
```

Related Commands

Command	Description
dial peer voice	Enters dial peer configuration mode and defines a dial peer.
voiceport	Enables a PLAR connection for an analog phone.

sccp switchback timeout guard

To set the Skinny Client Control Protocol (SCCP) switchback guard timer, use the **sccp switchback timeout guard** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp switchback timeout guard *seconds*

no sccp switchback timeout guard

Syntax Description

seconds	Guard timer value, in seconds. Range is from 180 to 7200. Default is 1200.

Command Default

1200 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

You can use the guard timer value for the switchback algorithm that follows the Graceful Timer method.

Examples

The following example sets the switchback guard timer value to 180 seconds (3 minutes):

```
Router# sccp switchback timeout guard 180
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

scenario-cause

To configure new Q.850 call-disconnect cause codes for use if an H.323 call fails, use the **scenario-cause** command in H.323-voice-service configuration mode. To revert to the defaults, use the **no** form of this command.

scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**} *code-id*}

no scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**}}

Syntax Description

arj-default	Q.850 call-disconnect cause code for use if a call fails for reasons that are assigned to the Admission Reject (ARJ) default cause code.
timeout arq	Q.850 call-disconnect cause code for use if the H.323 gatekeeper Automatic Repeat Request (ARQ) timer expires.
timeout t301	Q.850 call-disconnect cause code for use when the H.225 alerting (T301) timer expires. .
timeout t303	Q.850 call-disconnect cause code for use when the H.225 setup (T303) timer expires.
timeout t310	Q.850 call-disconnect cause code for use when the H.225 call-proceeding (T310) timer expires.
code-id	Q.850 code id number. Range: 1 to 127.

Command Default

No mapping occurs.

Command Modes

H.323-voice-service

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to configure new Q.850 call-disconnect cause codes for use if an H.323 voice call fails during setup.

Examples

The following example causes a gateway to send the default ARJ cause code of 24 rather than the previous default of 63 when a call fails for reasons that are associated with the ARJ default cause code:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# scenario-cause arj-default 24
```

Related Commands

Command	Description
h225 timeout call-proceeding	Sets the call-proceeding (T310, or call-setup to call-disconnect) disconnect timer.
map q850-cause	Maps a Q.850 call-disconnect cause code to a tone.
q850-cause	Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code.

sdspfarm tag

To permit a digital-signal-processor (DSP) farm to be to registered to Cisco Unified CME and associate it with the MAC address of a Skinny Client Control Protocol (SCCP) interface, use the **sdspfarm tag** command in telephony-service configuration mode. To delete a tag generated by the **sdspfarm tag** command, use the **no** form of this command.

sdspfarm tag *number device-name*

no sdspfarm tag *number device-name*

Syntax Description

number	Numeric name for a DSP farm. Number from 1 to 10.
device-name	Word describing the device, such as the MAC address, of the SCCP client interface that is preceded by the Message Transfer Part (MTP).

Command Default

DSP farm is not created.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The maximum number used to tag a DSP farm was increased to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. Use the **show interface** command to find the MAC address of the SCCP client interface.

Examples

The following example declares tag 1 as the MAC address of mac000a.8aea.ca80. The **show interface** command is used to obtain the MAC address.

```
Router# show interface FastEthernet 0/0
.
.
.
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000a.8aea.ca80 (bia 000a.8aea.ca80)
.
.
.
Router(config)# telephony-service
Router(config-telephony)# sdspfarm tag 1 mac000a.8aea.ca80
```

Related Commands

Command	Description
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.

sdspfarm transcode sessions

To specify the maximum number of transcoding sessions allowed per Cisco CallManager Express (Cisco CME) router, use the **sdspfarm transcode sessions** command in telephony-service configuration mode. To return to the default transcode session of 0, use the **no** form of this command.

sdspfarm transcode sessions *number*

no sdspfarm transcode sessions *number*

Syntax Description

number	Declares the number of DSP farm sessions. Valid values are numbers from 1 to 128.

Command Default

The default is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.

Usage Guidelines

The transcoding is allowed between G.711 and G.729. A session consists of two transcode streams. To configure this information, you must know how many digital-signal-processor (DSP) farms are configured on the network module (NM) farms in your Cisco CME router. DSP farms are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. To learn how many DSP farms have been configured on your Cisco CME router, use the **show sdspfarm** command.

Examples

The following example sets the maximum number of transcoding sessions allowed on the Cisco CME router to 20:

```
Router(config)# telephony-service
Router(config-telephony)# sdspfarm transcode sessions 20
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with an SCCP client interface's MAC address.
sdspfarm unit	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.
show sdspfarm	Displays the status of the configured DSP farms and transcoding streams.

sdspfarm units

To specify the maximum number of digital-signal-processor (DSP) farm profiles that are allowed to be registered to the Skinny Client Control Protocol (SCCP) server, use the **sdspfarm units** command in telephony-service configuration mode. To set the number of DSP farm profiles to the default value of 0, use the **no** form of this command.

sdspfarm units *number*

no sdspfarm units *number*

Syntax Description

number	Number of DSP farms. Valid values are numbers from 0 to 10.

Command Default

The default number is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The command increased support for the maximum number of DSP farms to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farm profiles do not include voice termination resources.

Examples

The following example configures a Cisco CME router to register one DSP farm:

```
Router(config)# telephony-service
Router(config-telephony)# sdspfarm units 1
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with the MAC address of an SCCP client interface.
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.

secondary

To set the backup location for storing call detail records (CDRs) if the primary location becomes unavailable, use the **secondary** command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

secondary {**ftp** *path/filename* **username** *username* **password** *password* | **ifs** *device***:***filename*}

no secondary {**ftp** | **ifs**}

Syntax Description

ftp *path/filename*	Name and location of the backup file on an external FTP server. Filename is limited to 25 characters.
ifs *device***:***filename*	Name and location of the backup file in flash memory or other internal file system on this router. Values depend on storage devices available on the router, for example flash or slot0. Filename is limited to 25 characters.
username *username*	User ID for authentication.
password *password*	Password user enters for authentication.

Command Default

Call records are saved to **flash:cdr**.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command defines the backup location where accounting records are sent if the file transfer to the primary device fails. The file accounting process retries the primary device, defined with the **primary** command, up to the number of times defined by the **maximum retry-count** command before automatically switching over to the secondary device.

The secondary device is attempted only after the primary device fails after the defined number of retries. If the secondary device also fails, the system logs an error and the file accounting process stops.

To manually switch back to the primary device when it becomes available, use the **file-acct reset** command. The system does not automatically switch back to the primary device.

A syslog warning message is generated if flash becomes full.

The filename you assign is appended with the gateway hostname and time stamp at the time the file is created to make the filename unique. For example, if you specify the filename cdrtest1 on a router with the hostname cme-2821, a file is created with the name cdrtest1.cme-2821.2007_10_28T22_21_41.000, where 2007_10_28T22_21_41.000 is the time that the file was created.

Limit the filename you assign with this command to 25 characters, otherwise it could be truncated when the accounting file is created because the full filename, including the appended hostname and timestamp, is limited to 63 characters.

Examples

The following example shows the backup location of the accounting file is set to flash:cdrtest2:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct reset	Manually switches back to the primary device for file accounting.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device.
primary	Sets the primary location for storing the CDRs generated for file accounting.

security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

security {**any** | **h323-id** | **e164**} {**password** default *password* | **password** separator *character*}

no security {**any** | **h323-id** | **e164**} {**password** default *password* | **password** separator *character*}

Syntax Description

any	Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, to identify the user to RADIUS/TACACS+.
h323-id	Uses the first H.323 ID type alias to identify the user to RADIUS/TACACS+.
e164	Uses the first E.164 address type alias to identify the user to RADIUS/TACACS+.
password default *password*	Default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
password separator *character*	Character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password are stripped from the string before it is treated as an H.323-ID alias to be registered. Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password are understood to be a password mechanism and no H.323-ID is registered.

Command Default

No default

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Use this command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint is not allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type is identified. If no alias of the proper type is found, the registration is rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. Although the **no security password** command undefines the password mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example enables security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id
security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security h323-id
security password separator !
```

Now if a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security e164
security password separator !
```

Now if a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security acl

To configure access-list based filtering on the gatekeeper, use the **security acl** command in gatekeeper configuration mode. To disable, use the no form of this command.

security acl {**answerarq**| **lrq**} *access-list-number*

no security acl {**answerarq**| **lrq**}

Syntax Description

answerarq	Filters incoming answer admission requests (AnswerARQ) using IP access-lists.
lrq	Filters incoming location requests (LRQs) using IP access-list.
access-list-number	Number of an access list that was configured using the **access-list** command. This is a decimal number from 1 to 99 or from 1300 to 1999. Only standard IP access lists numbered 1 through 99 are supported for the Tokenless Call Authorization feature.

Command Default

No default behavior or values.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.3(5)	This command was introduced.

Usage Guidelines

The **security acl** command configures the gatekeeper to use IP access lists for security. Use this command in conjunction with the **access-list** command to configure access-list based AnswerARQ and LRQ requests filtering on a gatekeeper. The gatekeeper will process only those requests which have been sent by sources that are permitted access by the specified IP access list. Requests sent by sources which have been denied by the specified IP access lists, will be rejected.

Examples

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 30 for call authorization:

```
Router(config-gk)# security acl answerarq 30
```

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 20 for LRQ filtering:

```
Router(config-gk)# security acl lrq 20
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

security izct

To configure the gatekeeper to include the destination E.164 alias in the IZC token hash, use the **security izct** command in gatekeeper configuration mode. To not include destination E.16 alias in IZC token hash, use the **no** form of this command.

security izct password {*password* [**hash** {**dest-alias | src-alias | dest-csa | src-csa | dest-epid | src-epid**}]}

no security izct {*password* [**hash** {**dest-alias | src-alias | dest-csa | src-csa | dest-epid | src-epid**}]}

Syntax Description

password *password*	Specifies the password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
hash	Specifies the options to be used in hash generation.
dest-alias	Specifies that the destination alias be included in hash generation.
src-alias	Specifies that the source alias be included in hash generation.
dest-csa	Specifies that the destination csa be included in hash generation.
src-csa	Specifies that the source alias be included in hash generation.
dest-epid	Specifies that the destination epid be included in hash generation.
src-epid	Specifies that the source epid be included in hash generation.

Command Default

Destination E.16 alias are not included in IZC token hash.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.4(15)XZ	The **dest-alias, src-alias, dest-csa, src-csa, dest-epid,** and **src-epid** keywords were added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configure the **security izct** command on the gatekeeper that generates the InterZone Clear Token (IZCT) hash to prevent rogue endpoints from sending an ARQ message with one called number and then changing the called number when they send the SETUP message to the terminating endpoint. When this command is configured, modification of the called number after the IZCT hash is generated by the trunking gateway will not be allowed. The IZCT token generated is valid only for 30 seconds and the IZCT hash token generated by terminating gatekeeper (TGK) can be used for multiple calls.

The call is rejected if any intermediate entity, such as a Cisco Gatekeeper Transaction Message Protocol (GKTMP) server (on the originating gatekeeper) or the originating gateway (using number translation rules), tries to modify the called number after the token is prepared during address resolution.

- The **hash** keyword at originating gateway (OGW) and TGK do not need to match.
- More than one **hash** keyword can be configured for the **security izct** command.

The **security izct** command must be configured at OGK or TGK in order to enable the feature.

When configuring an OGW to an OGK to a TGK and to a TGW. The **security izct** command is optional at the OGK, and required at the TGK. If hash parameter is not specified at the TGK, then dest-alias (default) will be used for hash token computation.

The **no** version of this command the requires the keyword argument combinations as defined in the preceding command syntax table.

Examples

The following example prevents modification of the called number after the IZCT hash is generated by the trunking gateway:

```
Router(config-gk)# security izct password example hash dest-alias
```

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security mode

To set the security mode for a specific dial peer using Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) services in a secure Cisco Unified CME network, use the **security mode** command in dial peer configuration mode. To return to the default, use the **no** form of this command.

security mode {**authenticated** | **none** | **encrypted** | **system**}

no security mode

Syntax Description

authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through the secure TLS connection on TCP port 2443.
none	SCCP signaling is not secure.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
system	Enables the security mode specified at the global level by the **stcapp security mode** command.

Command Default

Security mode specified at the global level is enabled.

Command Modes

Dial peer configuration (config-dialpeer)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify security mode on the voice gateway for Cisco Unified CME phone authentication and encryption.

Set the SCCP signaling security mode globally using the **stcapp security mode** command in global configuration mode. If you use both the **stcapp security mode** and the **security mode** commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example selects secure SCCP signaling in authenticated mode:

```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# security mode authenticated
```

The following example selects encrypted secure SCCP signaling and encryption through SRTP:

```
Router(config)# dial-peer voice 2 pots
Router(config-dialpeer)# security mode encrypted
```

Related Commands

Command	Description
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

sequence-numbers

To enable the generation of sequence numbers in each frame generated by the digital signal processor (DSP) for Voice over Frame Relay applications, use the **sequence-numbers** command in dial peer configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

sequence-numbers

no sequence-numbers

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

Sequence numbers on voice packets allow the digital signal processor (DSP) at the playout side to detect lost packets, duplicate packets, or out-of-sequence packets. This helps the DSP to mask out occasional drop-outs in voice transmission at the cost of one extra byte per packet. The benefit of using sequence numbers versus the cost in bandwidth of adding an extra byte to each voice packet on the Frame Relay network must be weighed to determine whether to disable this function for your application.

Another factor to consider is that this command does not affect codecs that require a sequence number, such as G.726. If you are using a codec that requires a sequence number, the DSP generates one regardless of the configuration of this command.

Examples

The following example disables generation of sequence numbers for VoFR frames for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 no sequence-numbers
```

Related Commands

Command	Description
called-number (dial peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.

Command	Description
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol (Voice over Frame Relay)	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

server (auto-config application)

To configure the IP address or name of the TFTP server for an auto-configuration application, use the **server** command in auto-config application configuration mode. To remove the IP address or name, use the **no** form of this command.

server *ip-address* | *domain-name* [*ip-address* | *domain-name*] [*ip-address* | *domain-name*]

no server

Syntax Description

ip-address	Specifies the IP address of the TFTP server.
domain-name	Specifies the domain name of the TFTP server.

Command Default

No default behavior or values.

Command Modes

Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **server** command used to configure two TFTP servers for an auto-configuration application:

```
Router(auto-config-app)# server 172.18.240.45 172.18.240.55
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the Skinny Client Control Protocol (SCCP) application.
show auto-config	Displays the current status of auto-config applications.

server (presence)

To specify the IP address of a presence server for sending presence requests from internal watchers to external presence entities, use the **server** command in presence configuration mode. To remove the server, use the **no** form of this command.

server *ip-address*

no server

Syntax Description

ip-address	IP address of the remote presence server.

Command Default

A remote presence server is not used.

Command Modes

Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command specifies the IP address of a presence server that handles presence requests when the watcher and presence entity (presentity) are not colocated. The router acts as the presence server and processes all presence requests and status notifications when a watcher and presentity are both internal. If a subscription request is for an external presentity, the request is sent to the remote server specified by this command.

Examples

The following example shows a presence server with IP address 10.10.10.1:

```
Router(config)# presence
Router(config-presence)# allow subscribe
Router(config-presence)# server 10.10.10.1
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
show presence global	Displays configuration information about the presence service.

Command	Description
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

server *name-tag*

no server *name-tag*

Syntax Description

name-tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Command Default Disabled

Command Modes RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines Each server can have multiple entries of IP addresses or aliases.

Examples The following example identifies the RLM server and defines the associated IP addresses:

```
rlm group 1
 server r1-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.

Command	Description
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

server absent reject

To configure the gatekeeper to reject new registrations or calls when the connection to the Gatekeeper Transaction Message Protocol (GKTMP) server is down, use the **server absent reject** command in gatekeeper configuration mode. To disable, use the **no** form of this command.

server absent reject {**arq** | **rrq**}

no server absent reject {**arq** | **rrq**}

Syntax Description

arq	Reject call admission request (ARQ) messages.
rrq	Reject registration request (RRQ) messages.

Command Default

By default, registrations and calls are not rejected.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660 and Cisco MC3810.

Usage Guidelines

This command configures the gatekeeper to reject new registrations or calls when it is unable to reach the GKTMP server because the TCP connection between the gatekeeper and GKTMP server is down. If multiple GKTMP servers are configured, the gatekeeper tries all of them and rejects registrations or calls only if none of the servers respond. You can also use this feature for security or service denial if a connection with the server is required to complete a registration.

Note This command assumes that RRQ and ARQ triggers are used between the gatekeeper and GKTMP server.

Examples

The following example directs the gatekeeper to reject registrations when it cannot connect to the GKTMP server:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 no shutdown
 server absent reject rrq
.
.
.
```

server flow-control

To enable flow control on the Cisco IOS gatekeeper (GK) and reset all thresholds to default, use the **server flow-control** command in gatekeeper configuration mode. To disable GK flow control, use the **no** form of this command.

server flow-control [**onset** *value*] [**abatement** *value*] [**qcount** *value*]

no server flow-control

Syntax Description

onset *value*	(Optional) Percentage of the server timeout value that is used to mark the server as usable or unusable. Range is from 1 to 100. The default is 80.
abatement *value*	(Optional) Percentage of the server timeout value that is used to mark the server as unusable or usable. Range is from 1 to 100. The default is 50. **Note** The abatement value must be less than the onset value.
qcount *value*	(Optional) Threshold length of the outbound queue on the GK. The queue contains messages waiting to be transmitted to the server. The TCP socket between the GK and Gatekeeper Transaction Message Protocol (GKTMP) server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches the qcount value, the server is marked unusable. Range is from 1 to 1000. The default is 400.

Command Default

The gatekeeper will send a maximum of 1000 RRQ messages.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Suppose the server timeout value is 3 seconds, the onset value is 50, and the abatement value is 40. When the average response time from the server to the Gatekeeper Transaction Message Protocol (GKTMP) reaches 1.5 seconds (the onset percentage of the server timeout value), the server is marked as unusable. During the period that the server is marked as unusable, REQUEST ALV messages are still sent to the unusable server. When the response time is lowered to 1.2 seconds (the abatement percentage of the timeout value), the server is marked usable again, and the GKTMP resumes sending messages to the server.

When the **server flow-control** command is configured on its own the default is value 400. If you change one parameter using the **server flow-control** command, all other parameters revert to the default values. For example, if the onset is configured at 70 percent and you use the **server flow-control** command to set the abatement level, the onset resets to the default (80 percent).

Examples

The following example uses the command with the default values:

```
Router# server flow-control
```

The following example enables the GKTMP Interface Resiliency Enhancement feature with an onset level of 50:

```
Router# server flow-control onset 50

*Mar  8 20:05:34.081: gk_srv_handle_flowcontrol: Flow control enabled

Router# show running-config

Building configuration...

Current configuration : 1065 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname snet-3660-3
!
.
.
.
gatekeeper
 zone local snet-3660-3 cisco.com
 zone remote snet-3660-2 cisco.com 209.165.200.225 1719
 zone prefix snet-3660-2 408*
 lrq forward-queries
 no use-proxy snet-3660-3 default inbound-to terminal
 no use-proxy snet-3660-3 default outbound-from terminal
 no shutdown
 server registration-port 8000
 server flow-control onset 50
!
.
.
.
end
```

The following example enables the GKTMP Interface Resiliency Enhancement feature:

```
Router# show gatekeeper status

Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        snet-3660-3
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:              unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

The following example shows the server statistics, including timeout encountered, average response time, and the server status:

```
Router# show gatekeeper server

            GATEKEEPER SERVERS STATUS
            =========================

Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 3.1

Gatekeeper-ID: Gatekeeper1
-------------------------
  RRQ  Priority: 5
    Server-ID: Server43
    Server IP address: 209.165.200.254:40118
    Server type: dynamically registered
    Connection Status: active
    Trigger Information:
      Trigger unconditionally

    Server Statistics:
    REQUEST RRQ Sent=0
    RESPONSE RRQ Received = 0
    RESPONSE RCF Received = 0
    RESPONSE RRJ Received = 0
    Timeout encountered=0
    Average response time(ms)=0
    Server Usable=TRUE
```

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

server registration-port

To configure the listener port for the server to establish a connection with the gatekeeper, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registration takes place, use the **no** form of this command.

server registration-port *port-number*

no server registration-port *port-number*

Syntax Description

port-number	Port number on which the gatekeeper listens for external server connections. Range is from 1 to 65535. There is no default.

Command Default No registration port is configured.

Note If the gatekeeper is to communicate with network servers, a registration port must be configured on it.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.2(11)T	This command was implemented on the Cisco 3700 series.

Usage Guidelines Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper.

Note The **no** form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples The following example establishes a listener port for a server connection with a gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server registration-port 20000
```

Related Commands

Command	Description
server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server routing

To specify the type of circuit messages sent to the Gatekeeper Transaction Message Protocol (GKTMP) server, use the **server routing** command in gatekeeper configuration mode. To return to the default, use the **no** form of this command.

server routing {**both** | **carrier** | **trunk-group**}

no server routing {**both** | **carrier** | **trunk-group**}

Syntax Description

both	Sends both types of information in GKTMP messages.
carrier	Sends only carrier information in GKTMP messages. This is the default.
trunk-group	Sends only trunk-group information in GKTMP messages.

Command Default Carrier

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to route carrier and trunk-group messages from the gatekeeper to the GKTMP server.

The **carrier** keyword sends the “I” and “J” tags in the GKTMP messages. The **trunk-group** keyword sends the “P” and “Q” tags in the GKTMP messages. The **both** keyword sends both sets of tags.

Examples The following example enables trunk-group information to be sent in GKTMP messages from the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server routing trunk-group
```

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger arq

To configure the admission request (ARQ) trigger statically on the gatekeeper, use the **server trigger arq** command in gatekeeper configuration mode. Submode commands are available after the **server trigger arq** command is entered. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of this command.

server trigger arq *gkid priority server-id server-ip-address server-port*

no server trigger arq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info-only	Use to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the Gatekeeper Transaction Message Protocol (GKTMP) server application.
shutdown	Use to temporarily disables a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send ARQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. • *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.

redirect-reason *reason-number*	Use to send ARQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*—Range is from 0 to 65535. Currently-used values are: – 0—Unknown reason. – 1—Call forwarding busy or called DTE busy. – 2—Call forwarded; no reply. – 4—Call deflection. – 9—Called DTE out of order. – 10—Call forwarding by the called DTE. – 15—Call forwarding unconditionally.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr** trigger was added.

Usage Guidelines Use this command and its optional submode commands to configure the admission request (ARQ) static server trigger. The gatekeeper checks incoming gateway ARQ messages for the configured trigger information. If an incoming ARQ message contains the specified trigger information, the gatekeeper sends the ARQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the ARQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the ARQ messages, the gatekeeper sends all ARQ messages to the GKTMP server application.

If the gatekeeper receives an ARQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming ARQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two ARQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two ARQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming ARQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one ARQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all ARQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_arqtrigger)# exit
```

The following example configures an ARQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any ARQ message that contains H.323 ID "3660-gw1", e-mail ID "joe.xyz.com", or a redirect reason 1. All other ARQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger arq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-arqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-arqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-arqtrigger)# redirect-reason 1
Router(config-gk-arqtrigger# exit
```

If the ARQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger arq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_arqtrigger)# destination-info e164 1800....
Router(config-gk_arqtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming ARQ messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the ARQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" ARQ trigger registration had been defined with a priority 1 instead of priority 2, the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those ARQ messages that contain a destination E.164 address that starts with 1800. All other ARQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger brq

To configure the bandwidth request (BRQ) trigger statically on the gatekeeper, use the **server trigger brq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger brq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger brq *gkid priority server-id server-ip-address server-port*

no server trigger brq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
redirect-reason *reason-number*	Use to send BRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*—Range is from 0 to 65535. Currently used values are as follows: – 0—Unknown reason. – 1—Call forwarding busy or called DTE busy. – 2—Call forwarded; no reply. – 4—Call deflection. – 9—Called DTE out of order. – 10—Call forwarding by the called DTE. – 15—Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This the command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr** trigger was added.

Usage Guidelines Use this command and its optional submode commands to configure the bandwidth request (BRQ) static server trigger. The gatekeeper checks incoming gateway BRQ messages for the configured trigger information. If an incoming BRQ message contains the specified trigger information, the gatekeeper sends the BRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the BRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the BRQ messages, the gatekeeper sends all BRQ messages to the GKTMP server application.

If the gatekeeper receives BRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming BRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two BRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two BRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming BRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one BRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all BRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger brq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_brqtrigger)# exit
```

The following example configures BRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any BRQ message containing redirect reason 1 or redirect reason 2. All other BRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger brq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-brqtrigger)# redirect-reason 1
Router(config-gk-brqtrigger)# redirect-reason 2
Router(config-gk-brqtrigger# exit
```

If the BRQ registration message defined above for gatekeeper “alpha” is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger brq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_brqtrigger)# redirect-reason 10
Router(config-gk_brqtrigger)# exit
```

Then gatekeeper “alpha” checks all incoming BRQ messages for redirect reasons 1 or 2 before checking for redirect reason 10. If any one of those conditions is met, the gatekeeper sends the BRQ message to the GKTMP server “Server-west”.

If the second gatekeeper “alpha” BRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper “alpha” would send to GKTMP server “Server-west” only those BRQ messages that contain a redirect reason 10. All other BRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger drq

To configure the disengage request (DRQ) trigger statically on the gatekeeper, use the **server trigger drq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger drq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger drq *gkid priority server-id server-ip-address server-port*

no server trigger drq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the Reliability, Availability, and Serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send automatic repeat request (ARQ) RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions: • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. • *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.

call-info-type { **fax** | **modem** | **voice**}	Use to send ARQ RAS messages containing a specified call info type to the GKTMP server application. The following types can be used: • **fax** • **modem** • **voice**
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.
12.4(4)T	The **call-info-type** submode command was added.

Usage Guidelines Use this command and its optional submode commands to configure the disengage request (DRQ) static server trigger. The gatekeeper checks incoming gateway DRQ messages for the configured trigger information. If an incoming DRQ message contains the specified trigger information, the gatekeeper sends the DRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the DRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the DRQ messages, the gatekeeper sends all DRQ messages to the GKTMP server application.

If the gatekeeper receives a DRQ trigger registration message that contains several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming DRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two DRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two DRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming DRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one DRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper together with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all DRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger drq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_drqtrigger)# exit
```

The following example configures DRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any DRQ message containing an H.323 ID "3660-gw1" or e-mail ID "joe.xyz.com". All other DRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger drq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-drqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-drqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-drqtrigger# exit
```

If the DRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger drq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_drqtrigger)# destination-info e164 1800....
Router(config-gk_drqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming DRQ messages for the destination H.323 ID or e-mail ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the DRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" DRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server Server-west only those DRQ messages that contain a destination E.164 address starting with 1800. All other DRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger irr

To configure the information request response (IRR) trigger statically on the gatekeeper, use the **server trigger irr** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger irr** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger irr *gkid priority server-id server-ip-address server-port*

no server trigger irr *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send IRR RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions: • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. – *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect-reason *reason-number*	Use to send IRR RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*—Range is from 0 to 65535. Currently used values are the following: – 0—Unknown reason. – 1—Call forwarding busy or called DTE busy. – 2—Call forwarded; no reply. – 4—Call deflection. – 9—Called DTE out of order. – 10—Call forwarding by the called DTE. – 15—Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr** trigger was added.

Usage Guidelines Use this command and its optional submode commands to configure the information request response (IRR) static server trigger. The gatekeeper checks incoming gateway IRR messages for the configured trigger information. If an incoming IRR message contains the specified trigger information, the gatekeeper sends the IRR message to the GKTMP server application. In addition, the IRR message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the IRR messages, the gatekeeper sends all IRR messages to the GKTMP server application.

If the gatekeeper receives an IRR trigger registration message that contains several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming IRR RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two IRR trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two IRR trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming IRR messages against the conditions on the higher priority registration

before using the lower priority registration. If the gatekeeper receives more than one IRR trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all IRR messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger irr sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_irrtrigger)# exit
```

The following example configures an IRR trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any IRR message containing an H.323 ID "3660-gw1", e-mail ID "joe.xyz.com, or a redirect reason 1. All other IRR messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger irr alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-irrtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-irrtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-irrtrigger)# redirect-reason 1
Router(config-gk-irrtrigger# exit
```

If the IRR registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger irr alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_irrtrigger)# destination-info e164 1800....
Router(config-gk_irrtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming IRR messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the IRR message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" IRR trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those IRR messages that contain a destination E.164 address starting with 1800. All other IRR messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lcf

To configure the location confirm (LCF) trigger statically on the gatekeeper, use the **server trigger lcf** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lcf** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger lcf *gkid priority server-id server-ip-address server-port*

no server trigger lcf *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional, and you may configure any of them, one per command line.

destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send LCF RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions: • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. – *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

remote-ext-address e164 *value*	Use to send LCF RAS messages that contain a specified remote extension address to the GKTMP server application. • **e164**—Remote extension address is an E.164 address. • *value*—Value against which to compare the destination address in the RAS messages. The following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr** trigger was added.

Usage Guidelines Use this command and its optional submode commands to configure the location confirm (LCF) static server trigger. The gatekeeper checks incoming gateway LCF messages for the configured trigger information. If an incoming LCF message contains the specified trigger information, the gatekeeper sends the LCF message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LCF message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LCF messages, the gatekeeper sends all LCF messages to the GKTMP server application.

If the gatekeeper receives an LCF trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LCF RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LCF trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LCF trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LCF messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LCF trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LCF messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lcf sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lcftrigger)# exit
```

The following example configures an LCF trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LCF message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a remote extension address starting with 1408. All other LCF messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lcf alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lcftrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lcftrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lcftrigger)# remote-ext-address e164 1408....
Router(config-gk-lcftrigger# exit
```

If the LCF registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lcf alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lcftrigger)# remote-ext-address e164 1800....
Router(config-gk_lcftrigger)# exit
```

then gatekeeper "alpha" checks all incoming LCF messages for the destination H.323 ID, e-mail ID, or remote extension address 1408 before checking for the remote extension address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LCF message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LCF trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LCF messages that contain a remote extension address E.164 address starting with 1800. All other LCF messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrj

To configure the location reject (LRJ) trigger statically on the gatekeeper, use the **server trigger lrj** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrj** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger lrj *gkid priority server-id server-ip-address server-port*

no server trigger lrj *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send LRJ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions: • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. • *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines Use this command and its optional submode commands to configure the location reject (LRJ) static server trigger. The gatekeeper checks incoming gateway LRJ messages for the configured trigger information. If an incoming LRJ message contains the specified trigger information, the gatekeeper sends the LRJ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRJ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRJ messages, the gatekeeper sends all LRJ messages to the GKTMP server application.

If the gatekeeper receives an LRJ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LRJ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRJ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRJ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRJ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LRJ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRJ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrj sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrjtrigger)# exit
```

The following example configures an LRJ trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LRJ message containing an H.323 ID "3660-gw1" or e-mail ID joe.xyz.com. All other LRJ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrj alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrjtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrjtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrjtrigger# exit
```

If the LRJ registration message defined above for gatekeeper “alpha” is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrj alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrjtrigger)# destination-info e164 1800....
Router(config-gk_lrjtrigger)# exit
```

then gatekeeper “alpha” checks all incoming LRJ messages for the destination H.323 ID or email ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRJ message to the GKTMP server “Server-west”.

If the second gatekeeper “alpha” LRJ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper “alpha” would send to GKTMP server “Server-west” only those LRJ messages that contain a destination E.164 address starting with 1800. All other LRJ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrq

To configure the location request (LRQ) trigger statically on the gatekeeper, use the **server trigger lrq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger lrq *gkid priority server-id server-ip-address server-port*

no server trigger lrq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination-info {**e164** | **email-id** | **h323-id**} *value*	Use to send LRQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions: • **e164**—Destination is an E.164 address. • **email-id**—Destination is an e-mail ID. • **h323-id**—Destination is an H.323 ID. • *value*—Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect-reason *reason-number*	Use to send LRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*—Range is from 0 to 65535. Currently used values are the following: – 0—Unknown reason. – 1—Call forwarding busy or called DTE busy. – 2—Call forwarded; no reply. – 4—Call deflection. – 9—Called DTE out of order. – 10—Call forwarding by the called DTE. – 15—Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines Use this command and its optional submode commands to configure the location request (LRQ) static server trigger. The gatekeeper checks incoming gateway LRQ messages for the configured trigger information. If an incoming LRQ message contains the specified trigger information, the gatekeeper sends the LRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRQ messages, the gatekeeper sends all LRQ messages to the GKTMP server application.

If the gatekeeper receives an LRQ trigger registration message that contains several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming LRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRQ messages against the conditions on the higher priority registration

before using the lower priority registration. If the gatekeeper receives more than one LRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrqtrigger)# exit
```

The following example configures an LRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any LRQ message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a redirect reason 1. Other LRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrqtrigger)# redirect-reason 1
Router(config-gk-lrqtrigger# exit
```

If the LRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrqtrigger)# destination-info e164 1800....
Router(config-gk_lrqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming LRQ messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LRQ messages that contain a destination E.164 address starting with 1800. All other LRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rai

To configure the resources available indicator (RAI) trigger statically on the gatekeeper, use the **server trigger rai** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rai** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger rai *gkid priority server-id server-ip-address server-port*

no server trigger rai *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint-type *value*	Use to send RAI RAS messages that contain a particular endpoint type to the GKTMP server application. • *value*—Value against which to compare the endpoint type in the RAS messages. Valid endpoint types are the following: – **gatekeeper**—Endpoint is an H.323 gatekeeper. – **h320-gateway**—Endpoint is an H.320 gateway. – **mcu**—Endpoint is a multipoint control unit (MCU). – **other-gateway**—Endpoint is another type of gateway not specified on this list. – **proxy**—Endpoint is an H.323 proxy. – **terminal**—Endpoint is an H.323 terminal. – **voice-gateway**—Endpoint is a voice gateway.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
supported-prefix *value*	Use to send RAI RAS messages that contain a specific supported prefix to the GKTMP server application. • *value*—Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr** trigger was added.

Usage Guidelines Use this command and its optional submode commands to configure the resources available indicator (RAI) static server trigger. The gatekeeper checks incoming gateway RAI messages for the configured trigger information. If an incoming RAI message contains the specified trigger information, the gatekeeper sends the RAI message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RAI message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RAI messages, the gatekeeper sends all RAI messages to the GKTMP server application.

If the gatekeeper receives an RAI trigger registration message that contains several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming RAI RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RAI trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RAI trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RAI messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RAI trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all RAI messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger rai sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_raitrigger)# exit
```

The following example configures an RAI trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any RAI message that contain an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other RAI messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rai alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-raitrigger)# endpoint-type mcu
Router(config-gk-raitrigger)# endpoint-type proxy
Router(config-gk-raitrigger)# supported-prefix 1#
Router(config-gk-raitrigger# exit
```

If the RAI registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rai alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_raitrigger)# supported-prefix 1234*
Router(config-gk_raitrigger)# exit
```

Then gatekeeper "alpha" checks all incoming RAI messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RAI message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" RAI trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those RAI messages that contain a supported prefix of 1234*. All other RAI messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rrq

To configure the registration request (RRQ) trigger statically on the gatekeeper, use the **server trigger rrq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rrq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger rrq *gkid priority server-id server-ip-address server-port*

no server trigger rrq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint-type *value*	Use to send RRQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value*—Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: – **gatekeeper**—Endpoint is an H.323 gatekeeper. – **h320-gateway**—Endpoint is an H.320 gateway. – **mcu**—Endpoint is a multipoint control unit (MCU). – **other-gateway**—Endpoint is another type of gateway not specified on this list. – **proxy**—Endpoint is an H.323 proxy. – **terminal**—Endpoint is an H.323 terminal. – **voice-gateway**—Endpoint is a voice gateway.
info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
supported-prefix *value*	Use to send RRQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value*—Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines Use this command and its optional submode commands to configure the registration request (RRQ) static server trigger. The gatekeeper checks incoming gateway RRQ messages for the configured trigger information. If an incoming RRQ message contains the specified trigger information, the gatekeeper sends the RRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RRQ messages, the gatekeeper sends all RRQ messages to the GKTMP server application.

If the gatekeeper receives an RRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming RRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper “sj.xyz.com” to send all RRQ messages to GKTMP server “Server-123”:

```
Router(config-gk)# server trigger rrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_rrqtrigger)# exit
```

The following example configures an RRQ trigger registration on gatekeeper “alpha”, which sends to the GKTMP server “Server-west” any RRQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other RRQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-rrqtrigger)# endpoint-type mcu
Router(config-gk-rrqtrigger)# endpoint-type proxy
Router(config-gk-rrqtrigger)# supported-prefix 1#
Router(config-gk-rrqtrigger# exit
```

If the RRQ registration message defined above for gatekeeper “alpha” is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_rrqtrigger)# supported-prefix 1234*
Router(config-gk_rrqtrigger)# exit
```

then gatekeeper “alpha” checks all incoming RRQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RRQ message to the GKTMP server “Server-west”.

If the second gatekeeper “alpha” RRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper “alpha” would send to GKTMP server “Server-west” only those RRQ messages that contain a supported prefix of 1234*. All other RRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger urq

To configure the unregistration request (URQ) trigger statically on the gatekeeper, use the **server trigger urq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger urq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger urq *gkid priority server-id server-ip-address server-port*

Submode Commands:

info-only
shutdown
endpoint-type *value*
supported-prefix *value*

no server trigger urq *gkid priority server-id server-ip-address server-port*

no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server-ip-address	IP address of the server.
server-port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Submode Commands

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint-type *value*	Use to send URQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value*—Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: – **gatekeeper**—Endpoint is an H.323 gatekeeper. – **h320-gateway**—Endpoint is an H.320 gateway. – **mcu**—Endpoint is a multipoint control unit (MCU). – **other-gateway**—Endpoint is another type of gateway not specified on this list. – **proxy**—Endpoint is an H.323 proxy. – **terminal**—Endpoint is an H.323 terminal. – **voice-gateway**—Endpoint is a voice gateway.

info-only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
supported-prefix *value*	Use to send URQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value*—Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default No trigger servers are set.

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines Use this command and its optional submode commands to configure the unregistration request (URQ) static server trigger. The gatekeeper checks incoming gateway URQ messages for the configured trigger information. If an incoming URQ message contains the specified trigger information, the gatekeeper sends the URQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the URQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the URQ messages, the gatekeeper sends all URQ messages to the GKTMP server application.

If the gatekeeper receives a URQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming URQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two URQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two URQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming URQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one URQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The the **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all URQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger urq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_urqtrigger)# exit
```

The following example configures a URQ trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any URQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other URQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger urq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-urqtrigger)# endpoint-type mcu
Router(config-gk-urqtrigger)# endpoint-type proxy
Router(config-gk-urqtrigger)# supported-prefix 1#
Router(config-gk-urqtrigger# exit
```

If the URQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger urq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_urqtrigger)# supported-prefix 1234*
Router(config-gk_urqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming URQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the URQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" URQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those URQ messages that contain a supported prefix of 1234*. All other URQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

service

To load and configure a specific, standalone application on a dial peer, use the **service** command in application configuration mode. To remove the application from the dial peer, use the **no** form of this command.

service [**alternate** | **default**] *service-name location*

no service [**alternate** | **default**] *service-name location*

Syntax Description

alternate	(Optional) Alternate service to use if the service that is configured on the dial peer fails.
default	(Optional) Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails.
service-name	Name that identifies the voice application. This is a user-defined name and does not have to match the script name.
location	Directory and filename of the Tcl script or VoiceXML document in URL format. For example, the following are valid locations: • built-in applications (builtin:*filename*) • flash memory (flash:*filename*) • HTTP server (http://../*filename*) • HTTPS (HTTP over Secure Socket Layer (SSL)) server (https://../*filename*) • TFTP server (tftp://../*filename*)

Command Default

The default service ("DEFAULT") is used if no other services are configured.

Command Modes

Application configuration (config-app)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(15)T	The *location* argument was modified to accept an HTTPS server URL. The description of the *location* argument was modified to describe how to specify the location for built-in applications.

Usage Guidelines

Use this command to load a service on the gateway. A service is a standalone application, such as a VoiceXML document or a Tcl script.

Examples

The following example shows a debitcard application configured on the dial peer.

```
Router(config)# application
Router(config-app)# service debitcard
tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
```

The following example shows the VoiceXML application myapp located on an HTTPS server configured on the dial peer.

```
Router(config)# application
Router(config-app)# service myapp https://myserver/myfile.vxml
```

The following example shows the auto-attendant (AA) service, called aa, which is a Tcl script embedded in the Cisco IOS software.

```
Router(config)# application
Router(config-app)# service queue builtin:app-b-acd
```

Related Commands

Command	Description
application (application configuration)	Configures an application on a dial peer.
call application alternate	Specifies an alternate application to use if the application that is configured in the dial peer fails.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.

service dsapp

To configure supplementary IP Centrex-like services for FXS phones on voice gateways to interwork with SIP-based softswitches, use the **service dsapp** command in the gateway-application configuration mode. Hookflash triggers a supplementary feature based on the current state of the call. To reset to the defaults, use the **no** form of this command.

service dsapp [*paramspace* **dialpeer** *dial-peer tag*] [*paramspace* **disc-toggle-time** *seconds*] [*paramspace* **callWaiting** *TRUE* | *FALSE*] [*paramspace* **callConference** *TRUE* | *FALSE*] [*paramspace* **blind-xfer-wait-time** *seconds*] [*paramspace* **callTransfer** *TRUE* | *FALSE*]

no service dsapp

Syntax Description

paramspace	Defines a package or service on the gateway, the parameters in that package or service become available for configuration when you use this argument.
dialpeer *dial-peer tag*	(Optional) Specifies the fixed dialpeer used to setup the call to the SIP server (trunk) side.
disc-toggle-time *seconds*	(Optional) Specifies the seconds to wait before switching to a call on hold if the active call disconnects. You can specify a range between 10 and 30 seconds.
callWaiting *TRUE* | *FALSE*	Toggles support for call waiting.
callConference *TRUE* | *FALSE*	Toggles support for call conferencing used to establish two calls with a single connection such that all three parties can talk together.
blind-xfer-wait-time *seconds*	Specifies the seconds to wait before triggering a blind call transfer. You can specify a range between 0 and 10 seconds. If you specify 0 seconds, no blind transfer call occurs.
callTransfer *TRUE* | *FALSE*	Toggles support for call transfers.

Command Defaults

If no supplementary features are defined, the defaults are as follows:

- **dialpeer**: -1
- **disc-toggle-time**: 10 seconds
- **callWaiting**: TRUE (enabled)
- **callConference**: TRUE (enabled)
- **blind-xfer-wait-time**: 0 seconds
- **callTransfer**: TRUE (enabled)

Command Modes

Gateway-application configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **service dsapp** command to configure supplementary Centrex-like features on FXS phones to interwork with SIP-based softswitches. Hookflash triggers supplementary features based on the current state of the call:

- Call Hold
- Call Waiting
- Call Transfer
- 3-Way Conference

Call Hold

Allows a call to be placed in a non-active state (with no media exchange). Table 38 summarizes the hookflash feature support for Call Hold.

Table 38 Call Hold Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Held call for remote party.	Second dial tone for FXS phone.
Call on hold	Hookflash	Active call.	FXS line connects to call.
Call on hold and active call	Hookflash	Active and held calls are swapped.	FXS line connects to previous held call.
	On hook	Active call is dropped.	Reminder ring on FXS line.
	Call on hold goes on hook	Call on hold is dropped.	None.
	Active call goes on hook	Active call is dropped	Silence.

Call Waiting

Allows a second call to be received while the phone is active with a call. Table 39 summarizes the hookflash feature support for Call Waiting.

Table 39 Call Waiting Hookflash Services

State	Action	Result	Response to FXS Line
Active call and waiting call	Hookflash.	Swap active call and waiting call.	FXS line connects to waiting call.
	Active call goes on hook.	Active call is disconnected.	Silence.
	Waiting call goes on hook.	Stay connected to active call.	None.
	On hook.	Active call is dropped.	Reminder ring on FXS line.

Call Transfer

With call transfer, you can do the following:

- Put an active call on hold while establishing a second call.

- Set up a call between two users
- Transfer calls by using these options
  - -Blind transfer
  - Semi-attended transfer
  - Attended transfer

Table 40 summarizes the hookflash feature support for Call Transfer.

Table 40 Call Transfer Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash.	Call is placed on hold.	Second dial tone.
Call on hold and outgoing dialed or alerting or active call	On hook.	Call on hold and active call.	
Call on hold and outgoing active call	Active call goes on hook.	Held call remains; active call dropped.	Silence.
Call on hold and outgoing active call	Call on hold goes on hook.	Active call remains; call on hold dropped.	None.
Call on hold and outgoing alerting call	Hookflash.	Active call dropped.	FXS line connects to previous held call.

3-Way Conference

Establishes two calls with a single connection, so that three parties can talk together. Table 41 summarizes the hookflash feature support for 3-way conferencing.

Table 41 3-Way Conference Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Call on hold.	Second dial tone.
Call on hold and active call		Join call on hold and active call.	Media mixing of both calls.

Examples

Enabling the DSApp Service

You can configure DSApp services either to a specific dial-peer, or globally to all dial peers. The following example shows the configuration to enable DSApp on a specific dial peer:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(conf-app)# dial-peer voice 1000 pots
Gateway(config-app)# service dsapp
```

The following example shows the configuration to enable DSApp globally on all dial peers:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# global
Gateway(config-app-global)# service default dsapp
```

Configuring Call Hold

The following example shows the configuration to enable the Call Hold feature:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param callHold TRUE
```

Configuring Call Waiting

The following example shows the configuration to enable the Call Waiting feature:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param callWaiting TRUE
```

Configuring Call Transfer

The following example shows the configuration to enable the Call Transfer feature:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param callTransfer TRUE
```

Configuring 3-Way Conferencing

The following example shows the configuration to enable the 3-Way Conferencing feature:

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param callConference TRUE
```

Configuring Disconnect Toggle Time

In this example, a disconnect toggle time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer after the originating call is placed on hook.

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param disc-toggle-time 10
```

Configuring Blind Transfer Wait Time

In this example, a blind transfer call wait time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer, after the originating call is placed on hook.

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param blind-xfer-wait-time 10
```

Configuring a Fixed Dial Peer Used for Outgoing Calls on SIP Trunk Side

In this example, a fixed dial peer is configured to set up a call to the SIP server (trunk) side.

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)# application
Gateway(config-app)# service dsapp
Gateway(config-app-param)# param dialpeer 5000
```

Related Commands

Command	Description
offer call-hold	Specifies the method of call hold on the gateway.

service-flow primary upstream

To assign a quality of service (QoS) policy to the data traveling between the cable modem and the multiple service operator (MSO) cable modem termination system (CMTS), use the **service-flow primary upstream** command in interface configuration mode. To disable the QoS policy, use the **no** form of this command.

service-flow primary upstream

no service-flow primary upstream

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is supported in the upstream direction only. Service flows are unidirectional.

Examples

The following example assigns a QoS policy to the data traveling between the cable modem and the MSO CMTS:

```
Router# configure terminal
Router(config)# interface Cable-Modem 0/2/0
Router(config-if)# service-flow primary upstream
```

service-relationship

To enter Annex G neighbor configuration mode and enable service relationships for the particular neighbor, use the **service-relationship** command in Annex G neighbor configuration mode. To exit this mode, use the **no** form of this command.

service-relationship

no service-relationship

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Annex G neighbor configuration

Command History

Release	Modification
12.2 (11)T	This command was introduced.

Usage Guidelines Service relationships are defined to be unidirectional. If a service relationship is established between border element A and border element B, A is entitled to send requests to B and to expect responses. For B to send requests to A and to expect responses, a second service relationship must be established. Repeat this command for each border-element neighbor that you configure.

Note The **no shutdown** command must be used to enable each service relationship.

Examples The following example enables a service relationship on a border element:

```
Router(config-annexg-neigh)# service-relationship
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time for which a border element attempts delivery.
shutdown	Enables or disables the border element.

service-type call-check

To identify preauthentication requests to the authentication, authorization, and accounting (AAA) server, use the **service-type call-check** command in AAA preauthentication configuration mode. To return this setting to the default, use the **no** form of this command.

service-type call-check

no service-type call-check

Syntax Description

This command has no arguments or keywords.

Command Default

The service type is not set to call-check.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Setting the service-type attribute to call-check causes preauthentication access requests to include this value, which allows AAA servers to distinguish preauthentication requests from other types of Access-Requests. This command has no effect on packets that are not of the preauthentication type.

Examples

The following example sets the RADIUS service-type attribute to call-check:

```
Router(config)# aaa preauth
Router(config-preauth)# service-type call-check
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

session

To associate a transport session with a specified session group, use the **session** command in backhaul session manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*

no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group-name	Session-group name.
remote-ip	Remote IP address.
remote-port	Remote port number. Range is from 1024 to 9999.
local-ip	Local IP address.
local-port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session-group. Range is from 0 to 9999; 0 is the highest priority.

Command Default No default behavior or values

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350 and Cisco AS5400 and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines It is assumed that the server is located on a remote machine.

Examples The following example associates a transport session with the session group “group5” and specifies the parameters:

```
Router(config-bsm)# session group group5 172.13.2.72 5555 172.18.72.198 5555 1
```

session group

To associate a transport session with a specified session group, use the **session group** command in backhaul session-manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*

no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group-name	Session-group name.
remote-ip	Remote IP address.
remote-port	Remote port number. Range is from 1024 to 9999.
local-ip	Local IP address.
local-port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session group. Range is from 0 to 9999; 0 has the highest priority.

Command Default No default behavior or values.

Command Modes Backhaul session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.

Usage Guidelines The Cisco VSC3000 server is assumed to be located on a remote machine.

Examples The following example associates a transport session with the session group named “group5” and specifies the keywords described above:

```
session group group5 172.16.2.72 5555 192.168.72.198 5555 1
```

session protocol (dial peer)

To specify a session protocol for calls between local and remote routers using the packet network, use the **session protocol** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**aal2-trunk | cisco | sipv2 | smtp**}

no session protocol

Syntax Description

aal2-trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
cisco	Dial peer uses the proprietary Cisco VoIP session protocol.
sipv2	Dial peer uses the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP). Use this keyword with the SIP option.
smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Command Default No default behaviors or values

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP peers on the Cisco 3600 series.
12.0(3)XG	This command was modified to support VoFR) dial peers.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300.
12.1(1)XA	This command was implemented for VoATM dial peers on the Cisco MC3810. The **aal2-trunk** keyword was added.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **sipv2** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco 7200 series. Supported for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. The **aal2-trunk** and **smtp** keywords are not supported on the Cisco 7200 series in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

The **cisco** keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco 7200 series router.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example shows that a VoIP dial peer for SIP has been configured as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session protocol (Voice over Frame Relay)

To establish a Voice over Frame Relay protocol for calls between the local and remote routers via the packet network, use the **session protocol** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**cisco-switched** | **frf11-trunk**}

no session protocol

Syntax Description

cisco-switched	Proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
frf11-trunk	FRF.11 session protocol.

Command Default **cisco-switched**

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP.
12.0(3)XG	This command was modified to support VoFR on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.0(4)T	The **cisco-switched** and **frf11-trunk** keywords were added for VoFR dial peers.

Usage Guidelines For Cisco-to-Cisco dial peer connections, Cisco recommends that you use the default session protocol because of the advantages it offers over a pure FRF.11 implementation. When connecting to FRF.11-compliant equipment from other vendors, use the FRF.11session protocol.

Note When using the FRF.11 session protocol, you must also use the **called-number** command.

Examples The following example configures the FRF.11 session protocol for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5552150
```

Related Commands

Command	Description
called-number (dial peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session protocol aal2

To enter voice-service-session configuration mode and specify ATM adaptation layer 2 (AAL2) trunking, use the **session protocol aal2** command in voice-service configuration mode.

session protocol aal2

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines This command applies to VoATM on theCisco 7200 series router.

In the voice-service-session configuration mode for AAL2, you can configure only AAL2 features, such as call admission control and subcell multiplexing.

Examples The following example accesses voice-service-session configuration mode, beginning in global configuration mode:

```
voice service voatm
 session protocol aal2
```

session protocol multicast

To set the session protocol as multicast, use the **session protocol multicast** command in dial peer configuration mode. To reset to the default protocol, use the **no** version of this command.

session protocol multicast

no session protocol multicast

Syntax Description

This command has no arguments or keywords.

Command Default

Default session protocol: Cisco.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced for the Cisco Hoot and Holler over IP application on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	This command was implemented on the Cisco 1750 and Cisco 1751.

Usage Guidelines

Use this command for voice conferencing in a hoot and holler networking implementation. This command allows more than two ports to join the same session simultaneously.

Examples

The following example shows the use of the **session protocol multicast** dial peer configuration command in context with its accompanying commands:

```
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:237.111.0.111:22222
 ip precedence 5
 codec g711ulaw
```

Related Commands

Command	Description
session target ipv4	Assigns the session target for voice-multicasting dial peers.

session refresh

To enable SIP session refresh globally, use the **session refresh** command in SIP configuration mode. To disable the session refresh, use the **no** form of this command.

session refresh

no session refresh

Syntax Description This command has no arguments or keywords.

Command Default No session refresh

Command Modes SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines Use the SIP **session refresh** command to send the session refresh request.

Examples The following example sets the session refresh under SIP configuration mode:

```
Router(conf-serv-sip)# Session refresh
```

Related Commands

Command	Description
voice-class sip session refresh	Enables session refresh at dial-peer level.

session start

To start a new instance (session) of a Tcl IVR 2.0 application, use the **session start** command in application configuration mode. To stop the session and remove the configuration, use the **no** form of this command.

session start *instance-name application-name*

no session start *instance-name*

Syntax Description

instance-name	Alphanumeric label that uniquely identifies this application instance.
application-name	Name of the Tcl application. This is the name of the application that was assigned with the **service** command.

Command Default No default behavior or values

Command Modes Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application session start** (global configuration) command.

Usage Guidelines

- This command starts a new session, or instance, of a Tcl IVR 2.0 application. It cannot start a session for a VoiceXML application because Cisco IOS software cannot start a VoiceXML application without an active call leg.
- You can start an application instance only after the Tcl application is loaded onto the gateway with the **service** command.
- If this command is used, the session restarts if the gateway reboots.
- If the application session stops running, it does not restart unless the gateway reboots. A Tcl script might intentionally stop running by executing a “call close” command for example, or it might fail because of a script error.
- You can start multiple instances of the same application by using different instance names.

Examples The following example starts a session named my_instance for the application named demo:

application

session start my_instance demo

The following example starts another session for the application named demo:

```
application
session start my_instance2 demo
```

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a Tcl IVR 2.0 application.
service	Loads a specific, standalone application on a dial peer.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

session target (MMoIP dial peer)

To designate an e-mail address to receive T.37 store-and-forward fax calls from a Multimedia Mail over IP (MMoIP) dial peer, use the **session target** command in dial peer configuration mode. To remove the target address, use the **no** form of this command.

session target mailto:{*name* | **d** | **m** | **e**}[@*domain-name*]

no session target

Syntax Description

mailto:	Matching calls are passed to the network using Simple Mail Transfer Protocol (SMTP) or Extended Simple Mail Transfer Protocol (ESMTP).
name	String that can be an e-mail address, name, or mailing list alias.
d	Macro that is replaced by the destination pattern of the gateway access number, which is the called number or dialed number identification service (DNIS) number.
m	Macro that is replaced by the redirecting dialed number (RDNIS) if present; otherwise, it is replaced by the gateway access number (DNIS). This macro requires use of the fax detection interactive voice response (IVR) application. **Note** Other strings can be passed to mailto in place of **m** if you modify the fax detection application Tool Command Language (TCL) script or VoiceXML document. For more information, refer to the readme file that came with the TCL script or the *Cisco VoiceXML Programmer's Guide*.
e	Macro that is replaced by the DNIS, the RDNIS, or a string that represents a valid e-mail address, as specified by the *cisco-mailtoaddress* variable in the transfer tag of the VoiceXML fax detection document. By default, if the *cisco-mailtoaddress* variable is not specified in the fax detection document, the DNIS is mapped to **e**. If **e** is not specified for the **session target mailto** command in the MMoIP dial peer, but the *cisco-mailtoaddress* variable is specified in the transfer tag of the fax detection document, then whatever is specified in the MMoIP dial peer takes precedence; the *cisco-mailtoaddress* variable is ignored. **Note** If a domain name is configured with this command, the VoiceXML document should pass only the username portion of the e-mail address and not the domain. If the domain name is passed from *cisco-mailtoaddress,* the **session target mailto** command should specify only **e**.
@*domain-name*	(Optional) String that contains the domain name to be associated with the target address, preceded by the at sign (@); for example, @*mycompany.com*.

Command Default

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(4)T	This command was modified to support store-and-forward fax.
12.1(5)XM1	The **m** keyword was introduced for the fax detection feature on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	The **e** keyword was introduced for VoiceXML fax detection on the Cisco AS5300.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to deliver e-mail to one recipient by specifying one e-mail name, or to deliver e-mail to multiple recipients by specifying an e-mail alias as the *name* argument and having that alias expanded by the mailer.

Use the **m** macro to include the redirecting dialed number (RDNIS) as part of the e-mail name when using the fax detection IVR application. If **m** is specified and RDNIS is not present in the call information, the access number of the gateway (the dialed number, or DNIS) is used instead. For example, if the calling party originally dialed 6015551111 to send a fax, and the call was redirected (forwarded on busy or no answer) to 6015552222 (the gateway), the RDNIS is 6015551111, and the DNIS is 6015552222.

Use the **e** macro to map the *cisco-mailtoaddress* variable in the VoiceXML fax detection document to the username portion of the e-mail address when sending a fax. If the VoiceXML document does not specify the *cisco-mailtoaddress* variable in the transfer tag, the application maps the DNIS to the e-mail address username.

Examples

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target mailto:marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running the sendmail application, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

The following example uses the fax detection IVR application. Here, the **session target** (MMoIP dial peer) command forwards fax calls to an e-mail account that uses the Redirected Dialed Number Identification Service (RDNIS) as part of its address. In this example, the calling party originally dialed 6015551111 to send a fax, and the call was forwarded (on busy or no answer) to 6015552222, which is the incoming number for the gateway being configured. The RDNIS is 6015551111, and the dialed number (DNIS) is 6015552222. When faxes are forwarded from the gateway, the session target in the example is expanded to 6015551111@mail-server.unified-messages.com.

```
dial-peer voice 4 mmoip
 session target mailto:$m$@mail-server.unified-messages.com
```

The following examples configure a session target for a VoiceXML fax detection application. In this example, the VoiceXML document passes just the username portion of the e-mail address, for example, "johnd":

```
dial-peer voice 4 mmoip
 session target mailto:$e$@cisco.com
```

In this example, the VoiceXML document passes the complete e-mail address including domain name, for example, "johnd@cisco.com":

```
dial-peer voice 5 mmoip
 session target mailto:$e$
```

Related Commands

Command	Description
destination-pattern	Specifies either the partial or full E.164 telephone number (depending on your dial plan) used to match the dial peer.
dial-peer voice	Enters dial peer configuration mode and defines a dial peer.

session target (POTS dial peer)

To designate loopback calls from a POTS dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

session target loopback:compressed | loopback:uncompressed

no session target

Syntax Description

loopback:compressed	All voice data is looped back in compressed mode to the source.
loopback:uncompressed	All voice data is looped back in uncompressed mode to the source.

Command Default

No loopback calls are designated.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and is supported on the Cisco AS5200, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

Examples

The following example loops back the traffic from the dial peer in compressed mode:

```
dial-peer voice 10 pots
 session target loopback:compressed
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.

session target (VoATM dial peer)

To specify a network-specific address for a specified VoATM dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 3600 Series Routers

session target *interface* **pvc** {*name* | *vpi*/*vci* | *vci*}

no session target

Cisco 7200 Series Routers

session target atm *slot*/*port* **pvc** {*word* | *vpi*/*vci* | *vci*} *cid*

no session target

Syntax Description

serial	Serial interface for the dial-peer address.
atm	ATM interface. The only valid number is 0.
interface	Interface type and interface number on the router.
slot/*port*	Slot and port numbers for the dial-peer address.
pvc	Specific ATM permanent virtual circuit (PVC) for this dial peer.
name	PVC name.
word	(Optional) Name that identifies the PVC. The argument can identify the PVC if a word identifier was assigned when the PVC was created.
vpi/*vci*	ATM network virtual path identifier (VPI) and virtual channel identifier (VCI) of this PVC. Values are as follows: • Cisco 3600 series with Multiport T1/E1 ATM network module with inverse multiplexing over ATM (IMA): *vpi* range is from 0 to 5; *vci* range is from 1 to 255. • OC3 ATM network module: *vpi* range is from 0 to 15; *vci* range is from 1 to 1023.
vci	ATM network virtual channel identifier (VCI) of this PVC.
cid	ATM network channel identifier (CID) of this PVC. Range is from 8 to 255.

Command Default Command is enabled with no IP address or domain name defined.

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.

Release	Modification
11.3(1)MA	This command was modified to support VoATM, VoHDLC, and POTS dial peers. The command was implemented on the Cisco MC3810.
12.0(3)XG	This command was modified to support VoFR dial peers. The command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to support VoATM and VoIP dial peers. The command was implemented on the Cisco 3600 series and the Cisco MC3810. Support for VoHDLC was removed.
12.1(1)XA	This command was modified to provide enhanced support for VoATM dial peers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol that you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

This command applies to on-ramp store-and-forward fax functions.

You must enter the **session protocol aal2-trunk** dial peer configuration command before you can specify a CID for a dial peer for VoATM on the Cisco 7200 series router.

Note This command does not apply to POTS dial peers.

Examples

The following example configures a session target for VoATM. The session target is sent to ATM interface 0 for a PVC with a VCI of 20.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm0 pvc 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

The following example configures a session target for VoATM. The session target is sent to ATM interface 0, and is for a PVC with a VPI/VCI of 1/100.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm1/0 pvc 1/100
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between local and remote routers via the packet network.
session target	Configures a network-specific address for a dial peer.
session target loopback	Tests the voice transmission path of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoFR dial peer)

To specify a network-specific address for a specified VoFR dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers

session target *interface dlci* [*cid*]

no session target

Cisco 7200 Series Routers

session target *interface dlci*

no session target

Syntax Description

interface	Serial interface and interface number (slot number and port number) associated with this dial peer. For the range of valid interface numbers for the selected interface type, enter a **?** character after the interface type.
dlci	Data link connection identifier for this dial peer. Range is from 16 to 1007.
cid	(Optional) DLCI subchannel to be used for data on FRF.11 calls. A CID must be specified only when the session protocol is **frf11-trunk**. When the session protocol is **cisco-switched**, the CID is dynamically allocated. Range is from 4 to 255. **Note** By default, CID 4 is used for data; CID 5 is used for call-control. We recommend that you select CID values between 6 and 63 for voice traffic. If the CID is greater than 63, the FRF.11 header contains an extra byte of data.

Command Default

The default for this command is enabled with no IP address or domain name defined.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was implemented for VoFR, VoHDLC, and POTS dial peers on the Cisco MC3810.
12.0(3)XG	This command was implemented for VoFR dial peers on the Cisco 2600 series and Cisco 3600 series. The *cid* option was added.
12.0(4)T	This command was integrated into Cisco IOS Release12.0(4)T and implemented for VoFR and POTS dial peers on the Cisco 7200 series.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

For VoFR dial peers, the *cid* option is not allowed when the **cisco-switched** option for the **session protocol** command is used.

Examples

The following example configures serial interface 1/0, DLCI 100 as the session target for Voice over Frame Relay dial peer 200 (an FRF.11 dial peer) using the FRF.11 session protocol:

```
dial-peer voice 200 vofr
 destination-pattern 13102221111
 called-number 5552150
 session protocol frf11-trunk
 session target serial 1/0 100 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoIP dial peer)

To designate a network-specific address to receive calls from a VoIP or VoIPv6 dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **sip-server** | **registrar**} [**:***port*]

no session target

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, and Cisco AS5850

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **settlement** *provider-number* | **sip-server** | **registrar**} [**:***port*]

no session target

Syntax Description

dhcp	Configures the router to obtain the session target via DHCP. **Note** The **dhcp** option can be made available only if the Session Initiation Protocol (SIP) is used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.
ipv4:*destination-address*	Configures the IP address of the dial peer to receive calls. The colon is required.
ipv6:[*destination-address*]	Configures the IPv6 address of the dial peer to receive calls. Square brackets must be entered around the IPv6 address. The colon is required.
dns:[s] *hostname*	Configures the host device housing the domain name system (DNS) server that resolves the name of the dial peer to receive calls. The colon is required. Use one of the following macros with this keyword when defining the session target for VoIP peers: • **s.**—(Optional) Source destination pattern is used as part of the domain name. • **d.**—(Optional) Destination number is used as part of the domain name. • **e.**—(Optional) Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. • **u.**—(Optional) Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. • *hostname*—String that contains the complete hostname to be associated with the target address; for example, serverA.example1.com.

enum:*table-num*	Configures ENUM search table number. Range is from 1 to 15. The colon is required.
loopback:rtp	Configures all voice data to loop back to the source. The colon is required.
ras	Configures the registration, admission, and status (RAS) signaling function protocol. A gatekeeper is consulted to translate the E.164 address into an IP address.
sip-server	Configures the global SIP server is the destination for calls from the dial peer.
:*port*	(Optional) Port number for the dial-peer address. The colon is required.
settlement *provider-number*	Configures the settlement server as the target to resolve the terminating gateway address. • The *provider-number* argument specifies the provider IP address.
registrar	Specifies to route the call to the registrar end point. • The **registrar** keyword is available only for SIP dial peers.

Command Default No IP address or domain name is defined.

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was modified. This command was implemented on the Cisco AS5300. The **ras** keyword was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **settlement** and **sip-server** keywords were added.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **enum** keyword was added.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(3)T	This command was modified. The **registrar** keyword was added.

Usage Guidelines

Use the **session target** command to specify a network-specific destination for a dial peer to receive calls from the current dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from the current dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial-peer session targets that you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, e-mail, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table** command in global configuration mode. The table is identified in the **session target enum** command with the *table-num* argument.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target dhcp** command to specify that the session target host is obtained via DHCP. The **dhcp** option can be made available only if the SIP is being used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

For the **session target settlement** *provider-number* command, when the VoIP dial peers are configured for a settlement server, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from the dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent (UA) configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

After the SIP endpoints are registered with the SIP registrar in the hosted unified communications (UC), you can use the **session target registrar** command to route the call automatically to the registrar end point. You must configure the **session target** command on a dial pointing towards the end point.

Examples

The following example shows how to create a session target using DNS for a host named “voicerouter” in the domain example.com:

```
dial-peer voice 10 voip
 session target dns:voicerouter.example.com
```

The following example shows how to create a session target using DNS with the optional **u**. macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading number 1310555. The optional **u**. macro directs the gateway to use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify a dial peer. The domain is “example.com.”

```
dial-peer voice 10 voip
 destination-pattern 1310555....
 session target dns:$u$.example.com
```

The following example shows how to create a session target using DNS, with the optional **d**. macro. In this example, the destination pattern has been configured to 13105551111. The optional macro **d**. directs the gateway to use the destination pattern to identify a dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 13105551111
 session target dns:$d$.example.com
```

The following example shows how to create a session target using DNS, with the optional **e**. macro. In this example, the destination pattern has been configured to 12345. The optional macro **e**. directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.example.com
```

The following example shows how to create a session target using an ENUM match table. It indicates that calls made using dial peer 101 should use the preferential order of rules in enum match table 3:

```
dial-peer voice 101 voip
 session target enum:3
```

The following example shows how to create a session target using DHCP:

```
dial-peer voice 1 voip
session protocol sipv2
voice-class sip outbound-proxy dhcp
session target dhcp
```

The following example shows how to create a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13105551111
 session target ras
```

The following example shows how to create a session target using settlement:

```
dial-peer voice 24 voip
 session target settlement:0
```

The following example shows how to create a session target using IPv6 for a host at 2001:10:10:10:10:10:10:230a:5090:

```
dial-peer voice 4 voip
destination-pattern 5000110011
session protocol sipv2
session target ipv6:[2001:0DB8:10:10:10:10:10:230a]:5090
codec g711ulaw
```

The following example shows how to configure Cisco Unified Border Element (UBE) to route a call to the registering end point:

```
dial-peer voice 4 voip
session target registrar
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session protocol (dial peer)	Specifies a session protocol for calls between local and remote routers using the packet network dial peer configuration mode.
settle-call	Specifies that settlement is to be used for the specified dial peer, regardless of the session target type.
sip-server	Defines a network address for the SIP server interface.
voice enum-match-table	Initiates the ENUM match table definition.

session transport

To configure a VoIP dial peer to use TCP or User Datagram Protocol (UDP) as the underlying transport layer protocol for Session Initiation Protocol (SIP) messages, use the **session transport** command in dial peer configuration mode. To reset to the default (**udp** keyword), use the **no** form of this command.

session transport {**system** | **tcp tls** | **udp**}

no session transport {**system** | **tcp tls** | **udp**}

Syntax Description

system	The SIP dial peer defers to the voice service VoIP session transport.
tcp tls	The SIP dial peer uses Transport Layer Security (TLS) over the TCP transport layer protocol.
udp	The SIP dial peer uses the UDP transport layer protocol. This is the default.

Command Default

UDP

Note The transport protocol specified with the **transport** command must match the one specified with this command.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(6)T	The **tls** keyword was added to the command.

Usage Guidelines

Use the **show sip-ua status** command to ensure that the transport protocol that you set using this command matches the protocol set using the **transport** command. The **transport** command is used in dial peer configuration mode to specify the SIP transport method, either UDP, TCP, or TLS over TCP.

Examples

The following example shows a VoIP dial peer configured to use TLS over TCP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport tcp tls
```

The following example shows a VoIP dial peer configured to use UDP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport udp
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session transport (H.323 voice-service)

To configure the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers, use the **session transport** command in H.323 voice service configuration mode. To reset the default value, use the **no** form of this command.

session transport {**udp** | **tcp** [**calls-per-connection** *value*]}

no session transport

Syntax Description

udp	Configures the H.323 dial peer to use the UDP transport layer protocol.
tcp	Configures the H.323 dial peer to use the TCP transport layer protocol. This is the default.
calls-per-connection	Configures the number of calls multiplexed into a single TCP connection.
value	The number of calls. The range is from 1 to 9999. The default is 5.

Command Default

TCP is the default session transport protocol; the default **calls-per-connection** value is 5.

Command Modes

H.323 voice service configuration

Command History

Release	Modification
12.2(1)T	This command was introduced for session initiation protocol (SIP) dial peers.
12.2(2)XA	This command was modified to include support for H323 dial peers and to include the **calls-per-connection** keyword.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows a dial peer configured to use the UDP transport layer protocol.

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# session transport udp
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

session transport (SIP)

To configure the underlying transport layer protocol for SIP messages to transport layer security over TCP (TLS over TCP) or User Datagram Protocol (UDP), use the session transport command in SIP configuration mode. To reset the value of this command to the default, use the **no** form of this command.

session transport {**udp** | **tcp tls**}

no session transport {**udp** | **tcp tls**}

Syntax Description

udp	Configure SIP messages to use the UDP transport layer protocol. This is the default.
tcp tls	Configure SIP messages to use the TLS over TCP transport layer protocol.

Command Default

The default for the command is UDP.

Command Modes

SIP configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced in SIP configuration mode.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
12.4(6)T	The **tls** keyword was added to the command.

Usage Guidelines

Use the **show sip-ua status** command to verify that the transport protocol set with the **session transport** command matches the protocol set using the **transport** command in SIP user agent configuration mode.

Examples

The following example configures the underlying transport layer protocol for SIP messages to UDP:

```
voice service voip
 sip
 session transport udp
```

The following example configures the underlying transport layer protocol for SIP messages to TLS over TCP:

```
voice service voip
 sip
 session transport tcp tls
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP gateway for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session-set

To create a Signlaing System 7 (SS7)-link-to-SS7-session-set association or to associate an SS7 link with an SS7 session set on the Cisco 2600-based Signaling Link Terminal (SLT), enter the **session-set** command in global configuration mode. To remove the link from its current SS7 session set and to add it to SS7 session set 0 (the default), use the **no** form of this command.

session-set *session-set-id*

no session-set

Syntax Description

session-set-id	SS7 session ID. Valid values are 0 and 1. Default is 0.

Command Default

SS7 session set 0

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced on the Cisco 2600-based SLT.

Usage Guidelines

On Cisco AS5350 and Cisco AS5400 platforms, the **channel-id** command is used to create an SS7-link-to-SS7-session-set association on the Cisco SLT. The Cisco 26xx platforms do not support the **channel-id** command, so channel IDs on the Cisco 26xx-based SLT are implicitly assigned on the basis of the slot location of the WAN interface card (WIC) and the channel group ID used to create the SS7 link.

If this command is omitted, the link is implicitly added to the SS7 session set 0, which is the default.

Examples

The following example shows how the **session-set** command is used to add the associated SS7 link to an SS7 session set:

```
session-set 1
```

The following example shows how the **no session-set** command is used to remove the link from its current SS7 session set and add it to SS7 session set 0, which is the default:

```
no session-set
```

Related Commands

Command	Description
channel-id	Assigns a session channel ID to a Signaling System 7 (SS7) serial link or assign an SS7 link to an SS7 session set on a Cisco AS5350 or Cisco AS5400.

set

To create a fault-tolerant or non-fault-tolerant session set with the client or server option, use the **set** command in backhaul session-manager configuration mode. To delete the set, use the **no** form of this command.

set *set-name* {**client** | **server**} {**ft** | **nft**}

no set *set-name* {**client** | **server**} {**ft** | **nft**}

Syntax Description

set-name	Session-set name.
client	The session set operates as a client. Select this option for signaling backhaul.
server	The session set operates as a server.
ft	Fault-tolerant operation. Select fault-tolerant if this session set can contain more than one session group, with each session group connecting the gateway to a different Cisco VSC3000. Fault-tolerance allows the system to operate properly if a session group in the session set fails.
nft	Non-fault-tolerant operation. Select non-fault-tolerant if this session set contains only one session group (which connects the gateway to a single Cisco VSC3000).

Command Default

No default behavior or values

Command Modes

Backhaul session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.

Usage Guidelines

Multiple session groups can be associated with a session set. For signaling backhaul, session sets should be configured to operate as clients. A session set cannot be deleted unless all session groups associated with the session set are deleted first.

Examples

The following example sets the client set named “set1” as fault-tolerant:

```
Router(config-bsm)# set set1 client ft
```

set http client cache stale

To set the status of all entries in the HTTP client cache to stale, use the **set http client cache stale** command in global configuration mode.

set http client cache stale

Syntax Description This command has no arguments or keywords.

Command Default Entries in the HTTP client cache are not marked stale manually.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use this command to force the HTTP client to check with the server to see if an updated version of the file exists when any cached entries are requested by the VoiceXML application. If the router is in nonstreaming mode, a conditional reload is sent to the HTTP server. If the router is in streaming mode, an unconditional reload is sent for the refresh. Regardless of which mode the router is in, the VoiceXML application is guaranteed to receive the most up-to-date file when you use the **set http client cache stale** command.

The **show http client cache** command shows a pound sign (#) next to the age of entries that are marked stale manually.

Examples The following example sets the status of all entries in the HTTP client cache to stale:

```
Router# set http client cache stale
```

Related Commands

Command	Description
show http client cache	Displays information about the entries contained in the HTTP client cache.

set pstn-cause

To map an incoming PSTN cause code to a Session Initiation Protocol (SIP) error status code, use the **set pstn-cause** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

set pstn-cause *value* **sip-status** *value*

no set pstn-cause

Syntax Description

pstn-cause *value*	PSTN cause code. Range is from 1 to 127
sip-status *value*	SIP status code that is to correspond with the PSTN cause code. Range is from 400 to 699.

Command Default

The default mappings defined in the following table are used:

Table 42 Default PSTN Cause Codes Mapped to SIP Events

PSTN Cause Code	Description	SIP Event
1	Unallocated number	404 Not found
2	No route to specified transit network	404 Not found
3	No route to destination	404 Not found
17	User busy	486 Busy here
18	No user responding	480 Temporarily unavailable
19	No answer from the user	
20	Subscriber absent	
21	Call rejected	403 Forbidden
22	Number changed	410 Gone
26	Non-selected user clearing	404 Not found
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal, unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	503 Service unavailable
41	Temporary failure	503 Service unavailable
42	Switching equipment congestion	503 Service unavailable
47	Resource unavailable	503 Service unavailable
55	Incoming class barred within the Closed User Group (CUG)	403 Forbidden

Table 42 Default PSTN Cause Codes Mapped to SIP Events (continued)

PSTN Cause Code	Description	SIP Event
57	Bearer capability not authorized	403 Forbidden
58	Bearer capability not currently available	501 Not implemented
65	Bearer capability not implemented	501 Not implemented
79	Service or option not implemented	501 Not implemented
87	User not member of the Closed User Group (CUG)	503 Service unavailable
88	Incompatible destination	400 Bad request
95	Invalid message	400 Bad request
102	Recover on Expires timeout	408 Request timeout
111	Protocol error	400 Bad request
Any code other than those listed above		500 Internal server error

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for on the Cisco AS5300 Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines

A PSTN cause code can be mapped only to one SIP status code at a time.

Examples

The following example maps a SIP status code to correspond to a PSTN cause code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set pstn-cause 111 sip-status 400
Router(config-sip-ua)# exit
```

Related Commands

Command	Description
set sip-status	Sets an incoming SIP error status code to a PSTN release cause code.

set sip-status

To map an incoming Session Initiation Protocol (SIP) error status code to a PSTN cause code, use the **set sip-status** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

set sip-status *value* **pstn-cause** *value*

no set sip-status

Syntax Description

sip-status *value*	SIP status code. Range is from 400 to 699.
pstn-cause *value*	PSTN cause code that is to correspond with the SIP status code. Range is from 1 to 127.

Command Default

The default mappings defined in the following table are used:

Table 43 Default SIP Events Mapped to PSTN Cause Codes

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking, unspecified
401 Unauthorized	57	Bearer capability not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer capability not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking, unspecified
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on Expires timeout
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking, unspecified
413 Request entity too long		
414 Request URI (URL) too long		
415 Unsupported media type	79	Service or option not available
420 Bad extension	127	Interworking, unspecified
480 Temporarily unavailable	18	No user response
481 Call leg does not exist	127	Interworking, unspecified
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete

Table 43 Default SIP Events Mapped to PSTN Cause Codes (continued)

SIP Event	PSTN Cause Code	Description
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
487 Request canceled	127	Interworking, unspecified
488 Not acceptable here	127	Interworking, unspecified
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option unavailable
504 Gateway timeout	102	Recover on Expires timeout
505 Version not implemented	127	Interworking, unspecified
580 Precondition failed	47	Resource unavailable, unspecified
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer capability not currently available

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines

A SIP status code can be mapped to many PSTN cause codes. For example, 503 can be mapped to 34, 38, and 58.

Examples

The following example maps a PSTN cause code to correspond to a SIP status code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set sip-status 400 pstn-cause 16
```

Related Commands

Command	Description
set pstn-cause	Sets an incoming PSTN cause code to a SIP error status code.

settle-call

To force a call to be authorized with a settlement server that uses the address resolution method specified in the **session target** command, use the **settle-call** command in dial peer configuration mode. To ensure that no authorization is performed by a settlement server, use the **no** form of this command.

settle-call *provider-number*

no settle-call *provider-number*

Syntax Description

provider-number	Digit defining the ID of a particular settlement server. The only valid entry is 0. **Note** If **session target** *type* is **settlement**, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Command Default

No default behavior or values.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

With the **session target** command, a dial peer can determine the address of the terminating gateway through the **ipv4**, **dns**, **ras**, and **settlement** keywords.

If the session target is not **settlement,** and the *settle-call provider-number* argument is set, the gateway resolves address of the terminating gateway using the specified method and then requests the settlement server to authorize that address and create a settlement token for that particular address. If the server cannot authorize the terminating gateway address suggested by the gateway, the call fails.

Do not combine the session target types **ras** and **settle-call**. Combination of session target types is not supported.

Examples

The following example sets a call to be authorized with a settlement server that uses the address resolution method specified in the **session target**:

```
dial-peer voice 10 voip
 destination-pattern 1408.......
 session target ipv4:172.22.95.14
 settle-call 0
```

Related Commands

Command	Description
session target	Specifies a network-specific address for a specified dial peer.

settlement

To enter settlement configuration mode and specify the attributes specific to a settlement provider, use the **settlement** command in global configuration mode. To disable the settlement provider, use the **no** form of this command.

settlement *provider-number*

no settlement *provider-number*

Syntax Description

provider-number	Digit that defines a particular settlement server. The only valid entry is 0.

Command Default 0

Command Modes Global configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines The variable *provider-number* defines a particular settlement provider. For Cisco IOS Release 12.1, only one clearinghouse per system is allowed, and the only valid value for *provider-number* is 0.

Examples This example enters settlement configuration mode:

```
settlement 0
```

Related Commands

Command	Description
connection-timeout	Configures the length of time for which a connection is maintained after a communication exchange is completed.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

settlement roam-pattern

To configure a pattern that must be matched to determine if a user is roaming, use the **settlement roam-pattern** command in global configuration mode. To delete a particular pattern, use the **no** form of this command.

settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}

no settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}

Syntax Description

provider-number	Digit defining the ID of particular settlement server. The only valid entry is 0.
pattern	User account pattern.
roaming	Specifies that a user is roaming.
noroaming	Specifies that a user is not roaming.

Command Default No default pattern is configured.

Command Modes Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines Multiple roam patterns can be entered on one gateway.

Examples The following example shows how to configure a pattern that determines if a user is roaming:

```
settlement 0 roam-pattern 1222 roaming
settlement 0 roam-pattern 1333 noroaming
settlement 0 roam-pattern 1444 roaming
settlement 0 roam-pattern 1555 noroaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settlement	Enters settlement configuration mode.

sgcp

To start and allocate resources for the Simple Gateway Control Protocol (SGCP) daemon, use the **sgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and kill the SGCP daemon, use the **no** form of this command.

sgcp

no sgcp

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP daemon is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

When the SGCP daemon is not active, all SGCP messages are ignored.

When you enter the **no sgcp** command, the SGCP process is removed.

Note After you enter the **no sgcp** command, you must save the configuration and reboot the router for the disabling of SGCP to take effect.

Examples

The following example enables the SGCP daemon:

```
sgcp
```

The following example disables the SGCP daemon:

```
no sgcp
```

Related Commands

Command	Description
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp call-agent

To define the IP address of the default Simple Gateway Control Protocol (SGCP) call agent in the router configuration file, use the **sgcp call-agent** command in global configuration mode. To remove the IP address of the default SGCP call agent from the router configuration, use the **no** form of this command.

sgcp call-agent *ipaddress* [*:udp port*]

no sgcp call-agent *ipaddress*

Syntax Description

ipaddress	IP address or hostname of the call agent.
:udp port	(Optional) UDP port of the call agent.

Command Default

No IP address is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

This command defines the IP address of the default SGCP call agent to which the router sends an initial RSIP (Restart In Progress) packet when the router boots up. This is used for initial bootup only before the SGCP call agent contacts the router acting as the gateway.

When you enter the **no sgcp call-agent** command, only the IP address of the default SGCP call agent is removed.

Examples

The following example enables SGCP and specifies the IP address of the call agent:

```
sgcp
sgcp call-agent 209.165.200.225
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp graceful-shutdown

To block all new calls and gracefully terminate all existing calls (wait for the caller to end the call), use the **sgcp graceful-shutdown** command in global configuration mode. To unblock all calls and allow new calls to go through, use the **no** form of this command.

sgcp graceful-shutdown

no sgcp graceful-shutdown

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until users terminate them, or until you enter the **no sgcp** command. When the last active call is terminated, the SGCP daemon is terminated, and all resources allocated to it are released.

Examples The following example blocks all new calls and terminates existing calls:

```
sgcp graceful-shutdown
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.

Command	Description
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp max-waiting-delay

To set the Simple Gateway Control Protocol (SGCP) maximum waiting delay to prevent restart avalanches, use the **sgcp max-waiting-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp max-waiting-delay *delay*

no sgcp max-waiting-delay *delay*

Syntax Description

delay	Maximum waiting delay (MWD), in milliseconds. Range is from 0 to 600000. Default is 3000.

Command Default 3,000 ms

Command Modes Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300, and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Examples The following example sets the maximum wait delay value to 40 ms:

```
sgcp max-waiting-delay 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp modem passthru

To enable Simple Gateway Control Protocol (SGCP) modem or fax pass-through, use the **sgcp modem passthru** command in global configuration mode. To disable SGCP modem or fax pass-through, use the **no** form of this command.

sgcp modem passthru {**ca** | **cisco** | **nse**}

no sgcp modem passthru {**ca** | **cisco** | **nse**}

Syntax Description

ca	Call-agent-controlled modem upspeed-method violation message.
cisco	Cisco-proprietary upspeed method based on the protocol.
nse	NSE-based modem upspeed method.

Command Default

SGCP modem or fax pass-through is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

You can use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions.

If you use the **nse** option, you must also configure the **sgcp tse payload** command.

Examples

The following example configures SGCP modem pass-through using the call-agent upspeed method:

```
sgcp modem passthru ca
```

The following example configures SGCP modem pass-through using the proprietary Cisco upspeed method:

```
sgcp modem passthru cisco
```

The following example configures SGCP modem pass-through using the NSE-based modem upspeed:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp quarantine-buffer disable

To disable the Simple Gateway Control Protocol (SGCP) quarantine buffer, use the **sgcp quarantine-buffer disable** command in global configuration mode. To reenable the SGCP quarantine buffer, use the **no** form of this command.

sgcp quarantine-buffer disable

no sgcp quarantine-buffer disable

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP quarantine buffer is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The SGCP quarantine buffer is the mechanism for buffering the SGCP events between two notification-request (RQNT) messages.

Examples

The following example disables the SGCP quarantine buffer:

```
sgcp quarantine-buffer disable
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request retries

To specify the number of times to retry sending notify and delete messages to the Simple Gateway Control Protocol (SGCP) call agent, use the **sgcp request retries** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request retries *count*

no sgcp request retries

Syntax Description

count	Number of times that a notify and delete message is retransmitted to the SGCP call agent before it is dropped. Range is from 1 to 100. Default is 3.

Command Default 3 times

Command Modes Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines The actual retry count may be different from the value you enter for this command. The retry count is also limited by the call agent. If there is no response from the call agent after 30 seconds, the gateway does not retry anymore, even though the number set using the **sgcp request retries** command has not been reached.

The router stops sending retries after 30 seconds, regardless of the setting for this command.

Examples The following example configures the system to send the **sgcp** command 10 times before dropping the request:

```
sgcp request retries 10
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request timeout

To specify how long the system should wait for a response to a request, use the **sgcp request timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request timeout *timeout*

no sgcp request timeout

Syntax Description

timeout	Time to wait for a response to a request, in milliseconds. Range is from 1 to 10000. Default is 500.

Command Default

500 ms

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

This command is used for “notify” and “delete” messages, which are sent to the SGCP call agent.

Examples

The following example configures the system to wait 40 ms for a reply to a request:

```
sgcp request timeout 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp restart

To trigger the router to send a Restart in Progress (RSIP) message to the Simple Gateway Control Protocol (SGCP) call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller, use the **sgcp restart** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp restart {**delay** *delay* | **notify**}

no sgcp restart {**delay** *delay* | **notify**}

Syntax Description

delay *delay*	Restart delay, in milliseconds. Range is from 0 to 600. Default is 0.
notify	Restarts notification upon the SGCP/digital interface state transition.

Command Default

0 ms

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to send RSIP messages from the router to the SGCP call agent. RSIP messages are used to synchronize the router and the call agent. RSIP messages are also sent when the **sgcp** command is entered to enable the SGCP daemon.

You must enter the **notify** option to enable RSIP messages to be sent.

Examples

The following example configures the system to wait 40 ms before restarting SGCP:

```
sgcp restart delay 40
```

The following example configures the system to send an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
sgcp restart notify
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp retransmit timer

To configure the Simple Gateway Control Protocol (SGCP) retransmission timer to use a random algorithm, use the **sgcp retransmit timer** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp retransmit timer {**random**}

no sgcp retransmit timer {**random**}

Syntax Description

random	SGCP retransmission timer uses a random algorithm.

Command Default

The SGCP retransmission timer does not use a random algorithm.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 3600 series and the Cisco MC3810 in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to enable the random algorithm component of the retransmission timer. For example, if the retransmission timer is set to 200 ms, the first retransmission timer is 200 ms, but the second retransmission timer picks up a timer value randomly between either 200 or 400. The third retransmission timer picks up a timer value randomly of 200, 400, or 800 as shown below:

- First retransmission timer: 200
- Second retransmission timer: 200 or 400
- Third retransmission timer: 200, 400, or 800
- Fourth retransmission timer: 200, 400, 800, or 1600
- Fifth retransmission timer: 200, 400, 800, 1600, or 3200 and so on.

After 30 seconds, the retransmission timer no longer retries.

Examples

The following example sets the retransmission timer to use a random algorithm:

```
sgcp retransmit timer random
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp timer

To configure how the gateway detects the Real-Time Transport Protocol (RTP) stream lost, use the **sgcp timer** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

no sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

Syntax Description

receive-rtcp *timer*	RTP Control Protocol (RTCP) transmission interval, in milliseconds. Range is from 1 to 100. Default is 5.
rtp-nse *timer*	RTP named signaling event (NSE) timeout, in milliseconds. Range is from 100 to 3000. Default is 200.

Command Default

receive-rtcp: 5 ms

rtp-nse: 200 ms

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The RTP NSE timer is used for proxy ringing (the ringback tone is provided at the originating gateway).

Examples

The following example sets the RTPCP transmission interval to 100 ms:

```
sgcp timer receive-rtcp 100
```

The following example sets the NSE timeout to 1000 ms:

```
sgcp timer rtp-nse 1000
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp tse payload

To enable Inband Telephony Signaling Events (TSE) for fax and modem operation, use the **sgcp tse payload** command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp tse payload *type*

no sgcp tse payload *type*

Syntax Description

type	TSE payload type. Range is from 96 to 119. Default is 0, meaning that the command is disabled.

Command Default

0 (disabled)

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload type.

If you set the **sgcp modem passthru** command to the **nse** value, then you must configure this command.

Examples

The following example sets Simple Gateway Control Protocol (SGCP) modem pass-through using the NSE-based modem upspeed and the Inband Telephony Signaling Events payload value set to 110:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.

Command	Description
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.up or down so that the call agent can synchronize
sgcp timer	Configures how the gateway detects the RTP stream host.

show aal2 profile

To display the ATM adaptation layer 2 (AAL2) profiles configured on the system, use the **show aal2 profile** command in privileged EXEC mode.

show aal2 profile {**all** {**itut** *profile-number* | **atmf** *profile-number* | **custom** *profile-number*}}

Syntax Description

all	Displays ITU-T, ATMF, and custom AAL2 profiles configured on the system.
itut	Displays ITU-T profiles configured on the system.
atmf	Displays ATMF profiles configured on the system.
custom	Displays custom profiles configured on the system.
profile-number	AAL2 profile number to display. Choices are as follows: For ITU-T: • 1 = G.711 u-law • 2 = G.711 u-law with silence insertion descriptor (SID) • 7 = G.711 u-law and G.729ar8 For ATMF: None. ATMF is not supported. For custom: • 100 = G.711 u-law and G.726r32 • 110 = G.711 u-law, G.726r32, and G.729ar8

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

This command applies to AAL2 VoATM applications on the Cisco 7200 series routers.

Examples

The following command displays all of the configured profiles in the system:

```
Router# show aal2 profile all

Printing all the Profiles in the system

Profile Type: ITUT Profile Number: 1 SID Support: 0
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: ITUT Profile Number: 2 SID Support: 1
Red enable: 1 Num entries: 1
```

```
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 100 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15

Profile Type: ITUT Profile Number: 7 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Coding type: g729ar8 Packet length: 10 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 110 SID Support: 1
Red enable: 1 Num entries: 3
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15
Coding type: g729ar8 Packet length: 30 UUI min: 8 UUI max: 15
```

Table 44 describes significant fields shown in this output.

Table 44 show aal2 profile all Field Descriptions

Field	Description
Coding type	Voice compression algorithm.
ITUT Profile Number	Predefined combination of one or more codec types configured for a digital signal processor (DSP).
Num entries	Number of profile elements.
Packet length	Sample size.
Profile Type	Category of codec types configured on DSP. Possible types are ITU-T, ATMF, and custom.
Red enable	Redundancy for type 3 packets.
SID Support	Silence insertion descriptor.
UUI max	Maximum sequence number on the voice packets.
UUI min	Minimum sequence number on the voice packets.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show atm video-voice address

To display the network service access point (NSAP) address for the ATM interface, enter the **show atm video-voice address** command in privileged EXEC mode.

show atm video-voice address

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to review ATM interface NSAP addresses that have been assigned with the **atm video aesa** command and to ensure that ATM management is confirmed for those addresses.

Examples

The following example displays ATM interface NSAP addresses:

```
Router# show atm video-voice address

nsap address                                    type         ilmi status
47.0091810000000002F26D4901.00107B4832E1.FE   VOICE_AAL5   Confirmed
47.0091810000000002F26D4901.00107B4832E1.C8   VIDEO_AAL1   Confirmed
```

Table 45 describes the significant fields shown in the output.

Table 45 show atm video-voice address Field Descriptions

Field	Description
NSAP address	NSAP address for the ATM interface.
Type	Type of ATM interface.
ILMI status	Integrated Local management Interface (ILMI) protocol status for the ATM interface.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show auto-config

To display the current status of auto-configuration applications, use the **show auto-config** command in privileged EXEC mode.

show auto-config [**application sccp**]

Syntax Description

application sccp	Displays the current status of only the Skinny Client Control Protocol (SCCP) application.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following is sample output from **show auto-config** command:

```
Router# show auto-config application sccp
 auto-config application: sccp
 auto-config admin state: ENABLED & ACTIVE
 download retries: (3)
 download timeout: no timeout, continuous retry
 server(s):  172.19.240.41 172.19.240.40 172.19.240.42
Configuration Download statistics:
        Download Attempted             : 2
          Download Successful          : 2
          Download Failed              : 0
        Configuration Attempted        : 2
          Configuration Successful     : 2
          Configuration Failed(parsing): 0
          Configuration Failed(config) : 0
Configuration Error History:
```

Table 46 describes the significant fields shown in the display.

Table 46 show auto-config Field Descriptions

Field	Description
ENABLED	Shows auto-config application: SCCP is enabled.
ACTIVE	Shows the SCCP application has registered to use auto-configuration.
timeout	Shows timeout is set to 0, continuous retry without timeout.

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
debug auto-config	Enables debugging for auto-configuration applications.
debug sccp config	Enables SCCP event debugging.

show backhaul-session-manager group

To display the status, statistics, or configuration for a particular session group or all available session groups, use the **show backhaul-session-manager group** command in privileged EXEC mode.

show backhaul-session-manager group {**status** | **stats** | **cfg**} {**all** | **name** *group-name*}

Syntax Description

status	Status for available session groups.
stats	Statistics for available session groups.
cfg	Configuration for available session groups.
all	Specified parameters for all session groups.
name *group-name*	A particular session group.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example displays statistics for all session groups:

```
Router# show backhaul-session-manager group stats all

Session-Group grp1 statistics
   Successful Fail-Overs      :0
   Un-Successful Fail-Over attempts:0
   Active Pkts receive count  :0
   Standby Pkts receive count :0
   Total PDUs dispatch err    :0
```

The following example displays the current configuration for all session groups:

```
Router# show backhaul-session-manager group cfg all

Session-Group
   Group Name :grp1
   Set Name   :set1
   Sessions   :3
    Dest:10.5.0.3 8304  Local:10.1.2.15 8304  Priority:0
    Dest:10.5.0.3 8300  Local:10.1.2.15 8300  Priority:2
    Dest:10.5.0.3 8303  Local:10.1.2.15 8303  Priority:2
    RUDP Options
      timer cumulative ack :100
      timer keepalive      :1000
      timer retransmit     :300
      timer transfer state :2000
      receive max          :32
      cumulative ack max   :3
      retrans max          :2
      out-of-sequence max  :3
      auto-reset max       :5
```

The following example displays the current state of all session groups. The group named “grp1” belongs to the set named “set1”.

```
Router# show backhaul-session-manager group status all

Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

Table 47 describes the significant fields shown in the output.

Table 47 show backhaul-session-manager group Field Descriptions

Field	Descrption
RUDP Options	Reliable User datagram Protocol (RUDP) options.
Status	One of the following: • Group-OutOfService—No session in the group has been established. • Group-Inservice—At least one session in the group has been established.
Status (use)	One of the following: • Group-Standby—The virtual switch controller (VSC) connected to the other end of this group goes into standby mode. • Group-Active—The VSC connected to the other end of this group is the active VSC. • Group-None—The VSC has not yet declared its intent.

Related Commands

Command	Description
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.
show backhaul-session-manager set	Displays session groups associated with a specific session set or all session sets.

show backhaul-session-manager session

To display various information about a session or sessions, use the **show backhaul-session-manager session** command in privileged EXEC mode.

show backhaul-session-manager session {**all** | **ip** *ip-address*}

Syntax Description

all	Information is displayed about all available sessions.
ip	Information is displayed about the session associated with this IP address only.
ip-address	IP address of the local or remote session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following command displays information for all available sessions:

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1  /*this session belongs to the group named 'grp1' */
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS,  /*see explanation below */
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
```

```
  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

Table 48 describes significant fields shown in this output.

Table 48 show backhaul-session-manager session Field Descriptions

Field	Description
State	Can be any of the following: • OPEN—The connection is established. • OPEN_WAIT—The connection is awaiting establishment. • OPEN_XFER—Session failover is in progress for this session, which is a transient state. • CLOSE—The session is down, also a transient state. The session waits a fixed amount of time and then moves to OPEN_WAIT.
Use-status	Indicates whether PRI signaling traffic is currently being transported over this session. Can be either of the following: • OOS—The session is not being used to transport signaling traffic. Out of service (OOS) does not indicate if the connection is established. • IS—The session is being used currently to transport all PRI signaling traffic. In service (IS) indicates that the connection is established.

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specific session group or all session groups.
show backhaul-session-manager set	Displays session groups associated with a specific session set or all session sets.

show backhaul-session-manager set

To display session groups associated with a specified session set or all session sets, use the **show backhaul-session-manager set** command in privileged EXEC mode.

show backhaul-session-manager set {**all** | **name** *session-set-name*}

Syntax Description

all	All available session sets.
name *session-set-name*	A specified session set.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following command displays session groups associated with all session sets:

```
Router# show backhaul-session-manager set all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specific session group or all session groups.
show backhaul-session-manager session	Displays status, statistics, or configuration of a session or all sessions.

show call accounting-template voice

To display accounting template activity, use the **show call accounting-template voice** command in privileged EXEC mode.

show call accounting-template voice [*acctTempName* | **master** | **qdump** | **summary**]

Syntax Description

acctTempName	(Optional) Name of the accounting template.
master	(Optional) Displays all vendor-specific attributes (VSAs) that are filtered by accounting templates.
qdump	(Optional) Displays template activity in the service and free queues.
summary	(Optional) Lists names of all the accounting templates and the number of attributes in each template currently being used.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- The **show call accounting-template voice** command displays the status and attributes defined in each template after it is configured.
- The **show call accounting-template voice** *acctTempName* command displays the status of a specific template and the attributes (VSAs) that are defined for that template.
- The **show call accounting-template voice master** command displays all VSAs that can be filtered by accounting templates.
- The **show call accounting-template voice qdump** command displays template activity in the service (svc) and free queues. It displays the template URL, the number of legs on which a template is active, and the state of a template.
  - After an accounting template is defined, it is put in the svc queue to serve new incoming calls. When a running accounting template is undefined or reloaded during an active call, the template is moved from the svc queue to the free queue and can be reused after all the active calls stop referencing it. Templates that are reloaded or undefined and that are referenced during an active call are considered to be in a “dirty” state and are called dirty templates.
  - To ensure that start and stop records correspond on an active call that is referencing a dirty template, all dirty templates must be kept alive until all active calls referencing that dirty template are released. After all active calls are released, the reloaded templates are applied to the next call.
- The **show call accounting-template voice summary** command displays the current status of all the accounting templates that are configured. It shows if the template was loaded and if it is running successfully.

Examples

The following example displays details about two templates named “cdr1” and “cdr2”.

```
Router# show call accounting-template voice

CDR template cdr1 is running
url: tftp://sanjoe/santa/abc/Templates/cdr1.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-gw-id (65)
attr:  subscriber (79)
attr:  in-portgrp-id (80)
attr:  out-portgrp-id (81)
Totally 6 attrs defined.

CDR template cdr2 is running
url: tftp://sanjoe/santa/abc/Templates/cdr2.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-connect-time (59)
attr:  h323-disconnect-time (64)
attr:  h323-gw-id (65)
attr:  h323-setup-time (76)
attr:  h323-voice-quality (78)
Totally 7 attrs defined.
```

The following example displays details about the template named “cdr1” only.

```
Router# show call accounting-template voice cdr1

CDR template cdr1 is running
url: tftp://sanjoe/santa/abc/Templates/cdr1.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-gw-id (65)
attr:  subscriber (79)
attr:  in-portgrp-id (80)
attr:  out-portgrp-id (81)
Totally 6 attrs defined.
```

The following example displays all 64 attributes that can be filtered by a template.

```
Router# show call accounting-template voice master

h323-call-origin
h323-call-type
h323-gw-id
h323-setup-time
h323-connect-time
h323-disconnect-time
h323-disconnect-cause
.
.
.
calling-party-category
originating-line-info
charge-number
transmission-medium-req
redirecting-number
backward-call-indicators
Totally 64 attributes are filterable.
```

The following example displays template activity in the service queue. Initially, no templates are in the dirty state.

```
Router# show call accounting-template voice qdump

name         url                                 is_dirty   no_of_legs
=========================================================================
cdr1         tftp://sanjoe/santa/abc                        0
cdr2         tftp://sanjoe/santa/abc                        0
cdr3         tftp://sanjoe/santa/abc                        0
```

After the templates are reloaded during active calls, the display below shows the templates named “cdr1” and “cdr2” to be in a dirty state.

```
.
.
.
Templates in freeq
cdr1         tftp://sanjoe/santa/abc            dirty       1
cdr2         tftp://sanjoe/santa/abc            dirty       1
```

The following example displays a summary of all configured accounting templates. The template named “cdr3” is not in running mode, either because it has been rejected or because it does not exist at the given URL.

```
Router# show call accounting-template voice summary

name         url                                      last_load  is_running
=========================================================================
cdr1         tftp://sanjoe/santa/abc                  success    is running
cdr2         tftp://sanjoe/santa/abc                  success    is running
cdr3         tftp://sanjoe/santa/abc                  fail       is not running
```

Table 49 describes the fields shown in the **show call accounting-template voice** display.

Table 49 show call accounting-template voice Field Descriptions

Field	Description
name	Name of the accounting template.
url	Location of the accounting template.
last_load	Describes if the accounting template was successfully or unsuccessfully loaded from its location.
is_running	Describes if the accounting template was activated after it was successfully loaded from its location.
is_dirty	Shows that the accounting template was reloaded during an active call.
no_of_legs	Number of call legs.
attr	Vendor-specific attributes (VSAs) defined in an accounting template.

Related Commands

Command	Description
gw-accounting aaa	Configures a new accounting template.

show call active fax

To display call information for T.37 store-and-forward fax transmissions in progress, use the **show call active fax** command in user EXEC or privileged EXEC mode.

show call active fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** *seconds* | **more** *seconds*}] | **id** *identifier*]

Syntax Description

brief	(Optional) Displays a truncated version of fax call information.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version of the fax call information.
duration	(Optional) Displays active calls that are longer or shorter than a specified *seconds* value. The arguments and keywords are as follows: • **less**—Displays calls shorter than the *seconds* value. • **more**—Displays calls longer than the *seconds* value. • *seconds*—Elapsed time, in seconds. Range is from 1 to 2147483647. There is no default value.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was modified. This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Release	Modification
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for T.37 store-and-forward fax calls currently connected through the router. This command works with both on-ramp and off-ramp store-and-forward fax functions.

To display information about fax relay calls in progress, use the **show call active voice** command.

Examples

The following is sample output from the **show call active fax** command:

```
Router# show call active fax

GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=peer one
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=1
RemoteIPAddress=10.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None
```

```
GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0
```

Table 50 provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command and a description of each field.

Table 50 show call active fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.

Table 50 show call active fax Field Descriptions (continued)

Field	Description
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds, at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
EchoCancellerMaxReflector=64	The location of the largest reflector, in milliseconds (ms). The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call, in ms.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.

Table 50 show call active fax Field Descriptions (continued)

Field	Description
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the time-division multiplexing (TDM) voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resourse Reservation Protocol (RSVP) quality of service (QoS) for this call.

Table 50 show call active fax Field Descriptions (continued)

Field	Description
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common channel signaling (CCS).
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active fax brief** command:

```
Router# show call active fax brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

1    : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1

1    : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms  noise:-1 acom:-1  i/0:0/0 dBm
```

The following is sample output from the **show call active fax** command displaying T.38 fax relay statistics:

```
Router# show call active fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
```

```
Total call-legs: 1

 GENERIC:
SetupTime=1874690 ms
Index=1
PeerAddress=5551234
PeerSubAddress=
PeerId=3
PeerIfIndex=244
LogicalIfIndex=118
ConnectTime=187875
CallDuration=00:00:44 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=309
TransmitBytes=5661
ReceivePackets=1124
ReceiveBytes=49189
TELE:
ConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
IncomingConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
CallID=1
Port=3/0/0 (1)
BearerChannel=3/0/0.1
TxDuration=2840 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitBufDepth 346
FaxRelayJitterBufOverflow 0
Initial HS Modulation is V.17/long/14400
Recent HS modulation is V.17/short/14400
Number of pages 1
Direction of transmission is Transmit
Num of Packets TX'ed/RX'ed 932/52
Packet loss conceal is 0
Encapsulation protocol is T.38 (UDPTL)
ECM is DISABLED
NoiseLevel=0
ACOMLevel=0
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=0
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=5551234
OriginalCallingOctet=0x80
OriginalCalledNumber=5555678
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=5551234
TranslatedCallingOctet=0x80
TranslatedCalledNumber=5555678
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=5555678
GwReceivedCalledOctet3=0x80
```

```
GwReceivedCallingNumber=5551234
GwReceivedCallingOctet3=0x80
GwReceivedCallingOctet3a=0x0
DSPIdentifier=1/0:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

Table 51 provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command for T.38 fax relay statistics and a description of each field.

Table 51 show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics

Field	Description
ACOMLevel	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, *General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers*. ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
ERLLevel	Current ERL level estimate in 0.1 dB increments.
FaxRate	Fax transmission rate from this peer to the specified dial peer, in bits per second (bps).
FaxRelayJitterBufOverflow	Fax relay jitter buffer overflow, in ms.
FaxRelayMaxJitBufDepth	Fax relay maximum jitter buffer depth, in ms.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call, in ms.
GwReceivedCalledNumber, GwReceivedCalledOctet3	Call information received at the gateway.
H323 call-legs	Type of call: H.323.
Initial HS Modulation	Initial high speed modulation used.
LogicalIfIndex	Index number of the logical interface for this call.
MGCP call-legs	Type of call: Media Gateway Control Protocol (MGCP).
Multicast call-legs	Type of call: Multicast.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, and octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
Port	Identification of the TDM voice port carrying the call.
Recent HS Modulation	Most recent high-speed modulation used.

Table 51 show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics (continued)

Field	Description
SIP call-legs	Type of call: SIP.
Telephony call-legs	Type of call: Telephony.
Total call-legs	Total calls.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalledNumber, TranslatedRedirectCalledOctet	Translated call information.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call, in ms.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show voice port	Displays configuration information about a specific voice port.

show call active media

To display call information for media calls in progress, use the **show call active media** command in user EXEC or privileged EXEC mode.

show call active media [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** *seconds* | **more** *seconds*}]]

Syntax Description

brief	(Optional) Displays a truncated version of call information.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. The range is a hexadecimal value from 1 to FFFF.
compact	(Optional) Displays a compact version of call information.
duration	(Optional) Displays the call history for the specified time duration.
less *seconds*	(Optional) Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
more *seconds*	(Optional) Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(18)M	This command was modified. The **less** keyword, **more** keyword, and *seconds* argument were added.

Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for media calls currently connected through the router.

When a media call is no longer active, its record is stored. You can display the record by using the **show call history media** command.

Examples

The following is sample output from the **show call active media** command:

```
Router# show call active media

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 2
Total call-legs: 2

 GENERIC:
```

```
SetupTime=408040 ms
Index=1
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
ConnectTime=408130 ms
CallDuration=00:00:01 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=57
ReceiveBytes=9120
VOIP-MEDIA:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=18
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=6B0CC055-C3511DB-801BC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
```

```
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
Source tg label=test5
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=4085254655
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=4085254655
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=

 GENERIC:
SetupTime=408050 ms
Index=1
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
```

```
ConnectTime=408160 ms
CallDuration=00:00:03 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=188
TransmitBytes=30080
ReceivePackets=0
ReceiveBytes=0
VOIP-MEDIA:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=19
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=6B0E94CD-C3511DB-801DC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=1495 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=95 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
```

```
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
Source tg label=test5
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=4085254655
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=4085254655
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 2
Total call-legs: 2
```

Table 50 describes the significant fields shown in the display.

Table 52 show call active media Field Descriptions

Field	Description
Telephony call-legs	Total telephony call legs for which call records are available.
SIP call-legs	Total session initiation protocol (SIP) call legs for which call records are available.
H323 call-legs	Total H.323 call legs for which call records are available.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR (for Frame Relay), or HDLC (for High-Level Data Link Control).
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
Index	Dial peer identification number.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
LogicalIfIndex	Index number of the logical interface for this call.
ConnectTime	Time, in milliseconds, at which the call was connected.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
InfoType	Information type for this call; for example, voice or fax.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
ReceivePackets	Number of packets received by this peer during this call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ConnectionId	Global call identifier for this gateway call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionTarget	Session target of the peer used for this call.

Table 52 show call active media Field Descriptions (continued)

Field	Description
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call, in ms.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call, in ms.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
InSignalLevel	Active input signal level from the telephony interface used by this call.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
ERLLevel	Current echo return loss (ERL) level for this call.
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
PeerSubAddress	Subaddress when this call is connected.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.

Related Commands

Command	Description
show call history media	Displays the call history table.

show call active video

To display call information for Signaling Connection Control Protocol (SCCP), Session Initiation Protocol (SIP), and H.323 video calls in progress, use the **show call active video** command in user EXEC or privileged EXEC mode.

show call active video [[**brief**] [**id** *call-identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **echo-canceller** *call-id* | **stats**]

Syntax Description

brief	(Optional) Displays a truncated version of active video call information.
id *call-identifier*	(Optional) Displays only the video calls with the specified identifier. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of active video call information.
duration	(Optional) Displays call history for the specified time duration.
less	Displays call history for shorter duration calls.
more	Displays call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
echo-canceller *call-id*	(Optional) Displays information about the state of the extended echo canceller (EC). The range is from 0 to FFFFFFFF.
stats	(Optional) Displays information about DSP statistics and video quality metrics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(4)XC	Cisco Unified CME 4.0	This command was introduced.
12.4(9)T	Cisco Unified CME 4.0	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(11)T	—	This command was modified. Support was added for SIP and H.323 calls.
12.4(16); 12.4(15)T	—	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
15.1(4)M	Cisco Unified CME 8.1	This command was modified. The **stats** keyword was added.

Usage Guidelines

Use this command to display the contents of the active video call table.

Before you can query the echo state, you need to know the hexadecimal ID. Use the **show call active video brief** command to find the hexadecimal ID.

Examples

The following is sample output from the **show call active video brief** command:

```
Router # show call active video brief

<ID>: <CallID> <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
   video: h320:<type> tx:<video codec> <video pkts>/<video bytes> rx:<video codec> <video
pkts>/<video bytes>
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 0
Total call-legs: 2

141D : 83 165385200ms.1 +3180 pid:6 Answer 2004 active
 dur 00:00:36 tx:1602/1232038768 rx:3237/1192797
 IP 192.0.2.0:5445 SRTP: off rtt:0ms pl:27980/0ms lost:0/0/0 delay:0/0/0ms g711ulaw
TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a

141D : 84 165385200ms.2 +3170 pid:20008 Originate 1008 active
 dur 00:00:36 tx:1698/271680 rx:1796/287360
 Tele 50/0/8 (84) [50/0/8.0] tx:33960/33960/0ms g711ulaw noise:0 acom:0  i/0:0/0 dBm

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 0
Total call-legs: 2
```

The following is sample output from the **show call active video** command:

```
Router# show call active video
Telephony call-legs: 4
SIP call-legs: 0
```

```
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 6

 GENERIC:
SetupTime=169281770 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=169281770 ms
CallDuration=01:20:44 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=819728
TransmitBytes=571031017
ReceivePackets=796308
ReceiveBytes=566120602

VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=85
GlobalCallId=[0x0 0x0 0x0 0x0]
CallReferenceId=25666520
CallServiceType=Video Conference
RTP Loopback Call=FALSE RemoteIPAddress=0.0.0.0
RemoteUDPPort=2000
RemoteSignallingIPAddress=0.0.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=1.4.211.39
RemoteMediaPort=2000
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
SafEnabled=FALSE
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
Video Conferee Statistics
ConfereeActualFrameRate=0
ConfereeActualBitrate=934600
ConfereeTotalRxPackets=129853
```

```
ConfereeTotalRxBytes=125825024
ConfereeTotalTxPackets=129853
ConfereeTotalTxBytes=125825085
ConfereeTotalPacketsDropped=313
ConfereeCurrentPacketsDropped=0
ConfereeTotalPacketsOutOfOrder=296
ConfereeCurrentPacketsOutOfOrder=0
ConfereeMaxJitter=0
ConfereeCurJitter=0
ConfereeMaxDelay=0
ConfereeCurDelay=0
ConfereeMaxOutOfSyncDelay=0
ConfereeCurrentOutOfSyncDelay=0
ConfereeFastVideoUpdateRate=0
ConfereeVideoDuration=1076
Video Quality Scores
RxVideoMOSInstant=78/100 (Good)
RxVideoMOSAverage=70/100 (Good)
VIDEO:
VideoTransmitCodec=H264
VideoTransmitPictureWidth=640
VideoTransmitPictureHeight=480
VideoTransmitFrameRate=30
VideoTransmitBitrate=934600 bps
VideoTransmitLevel=2
VideoTransmitProfile=Baseline
VideoTransmitPayloadFormat=RFC3984
VideoTransmitPackets=129853
VideoTransmitBytes=125825085
VideoTransmitDuration=1076 seconds
VideoReceiveCodec=H264
VideoReceivePictureWidth=640
VideoReceivePictureHeight=480
VideoReceiveFrameRate=30
VideoReceiveBitrate=934600 bps
VideoReceiveLevel=2
VideoReceiveProfile=Baseline
VideoReceivePayloadFormat=RFC3984
VideoReceivePackets=129853
VideoReceiveBytes=125825024
VideoReceiveDuration=1076 seconds
VideoCap_Codec=H264
VideoCap_Format=CUSTOM
VideoCap_PictureWidth=640
VideoCap_PictureHeight=480
VideoCap_FrameRate=30
VideoCap_Bitrate=960000 bps
VideoCap_Level=2
VideoCap_Profile=Baseline
VideoCap_PayloadFormat=RFC3984
VideoLostPackets=0
VideoEarlyPackets=0
VideoLatePackets=0
VideoUsedBandwidth=934600
VideoNumberOfChannels=0

PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
```

```
VAD = disabled
CoderTypeRate=h264
CodecBytes=0
Media Setting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=
MlppServiceDomainNW=0 (none)
MlppServiceDomainID=
PrecedenceLevel=0 (PRECEDENCE_LEVEL_NONE)
```

The following shows sample output from the **show call active video stats** command:

```
Router# show call active video stats

<ID>: <CallID> <start>ms.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 1
Multicast call-legs: 0
Total call-legs: 1
0    : 5 *10:54:50.661 PDT Tue Jan 11 2011.2 +0 pid:0 Originate  connecting
 dur 00:17:27 tx:126342/122451295 rx:126640/122453063

Video Conferee Statistics
ConfereeActualFrameRate=0  ConfereeActualBitrate=934300
ConfereeTotalRxPackets=126166  ConfereeTotalRxBytes=122282402
ConfereeTotalTxPackets=126166  ConfereeTotalTxBytes=122282463
ConfereeTotalPacketsDropped=295  ConfereeCurrentPacketsDropped=0
ConfereeTotalPacketsOutOfOrder=278  ConfereeCurrentPacketsOutOfOrder=0
ConfereeMaxJitter=0  ConfereeCurJitter=0
ConfereeMaxDelay=0  ConfereeCurDelay=0
ConfereeMaxOutOfSyncDelay=0  ConfereeCurrentOutOfSyncDelay=0
ConfereeFastVideoUpdateRate=0  ConfereeVideoDuration=1046

Video Quality Scores
RxVideoMOSInstant=78/100 (Good)
  (Compression Degradation: 86%, Network Degradation: 13%, Transcoding Degradation: 0%)
RxVideoMOSAverage=70/100 (Good)
  (Compression Degradation: 93%, Network Degradation: 6%, Transcoding Degradation: 0%)
```

Table 53 describes the significant fields shown in the display, in alphabetical order.

Table 53 show call active video Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of a second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) delay during this call, in ms.
Index	Dial peer identification number.

Table 53 show call active video Field Descriptions

Field	Description
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.

Table 53 show call active video Field Descriptions

Field	Description
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VideoCap_Annex	Extension of the video stream; for example, annex D1 and E.
VideoCap_Bitrate	Negotiated bitrate of the video stream; for example, 128000 b/s.
VideoCap_Codec	Codec for the active video call.
VideoCap_Format	Video format for the active video call.
VideoCap_FrameRate	Negotiated frame rate of the video stream; for example, 15 or 30 f/s.
VideoCap_PictureHeight	Height of the video resolution.
VideoCap_PictureWidth	Width of the video resolution.
VideoEarlyPackets	Number of early packets for a video call.
VideoLatePackets	Number of late packets in a video call.
VideoLostPackets	Number of lost packets in a video call.
VideoNumberOfChannels	Number of channels used for a video call.
Video Quality Score	Instantaneous and average Mean Opinion Score (MOS) for each active call leg. The MOS score is based on the amount of video quality degradation caused by compression distortion and the amount of video quality degradation caused by packet loss. The scale for the MOS score is as follows: • Excellent—(80—100) • Good—(60—80) • Fair—(40—60) • Poor—(20—40) • Bad—(0—20)
VideoReceiveBytes	Number of bytes received in the video call.
VideoReceiveCodec	Type of video codec used in the receiving stream.
VideoReceivePackets	Number of packets received in the video call.
VideoTransmitBytes	Number of bytes transmitted in the video call.
VideoTransmitCodec	Type of video codec used in the transmission stream.
VideoTransmitPackets	Number of packets transmitted in the video call.

Table 53 show call active video Field Descriptions

Field	Description
VideoUsedBandwidth	Bandwidth, in kbps, used for a video call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in milliseconds. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call history video	Displays call history information for SCCP video calls.

show call active voice

To display call information for voice calls in progress, use the **show call active voice** command in user EXEC or privileged EXEC mode.

show call active voice [[**brief**] [**long-dur-call-inactive** | **media-inactive**] [**called-number** *number* | **calling-number** *number*] [**id** *call-identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **echo-canceller** {*hexadecimal-id* | **port** *slot-number* | **summary**} | **long-dur-call** [**called-number** *number* | **calling-number** *number*] | **redirect tbct** | **stats**]

Syntax in Cisco IOS Release 12.2(33)SXH and Subsequent 12.2SX Releases

show call active [**brief**]

Syntax Description

brief	(Optional) Displays a truncated version of call information.
long-dur-call-inactive	(Optional) Displays long duration calls that are detected and notified.
media-inactive	(Optional) Displays information about inactive media that have been detected.
called-number *number*	(Optional) Displays a specific called number pattern.
calling-number *number*	(Optional) Displays a specific calling number pattern.
id *call-identifier*	(Optional) Displays only the call with the specified *call-identifier* value. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of call information.
duration	(Optional) Displays the call history for the specified time duration.
less *seconds*	Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
more *seconds*	Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.
echo-canceller	(Optional) Displays information about the state of the extended echo canceller (EC).
hexadecimal-id	The hexadecimal ID of an active voice call. The range is from 0x0 to 0xFFFFFFFF.
port *slot-number*	Displays EC details for a specified active voice port. The range varies depending on the voice ports available on the router.
summary	Displays an EC summary for all active voice calls.
long-dur-call	(Optional) Displays long duration calls that are detected and notified.
redirect	(Optional) Displays information about active calls that are being redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT).
tbct	Displays information about TBCT calls.
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(13)T	This command was modified. The **echo-canceller** keyword was added. The command output was modified with an extra reflector location when the extended EC is present; the largest reflector location is shown.
12.3(1)	This command was modified. The **redirect** keyword was added.
12.3(4)T	This command was modified. The **called-number**, **calling-number**, and **media-inactive** keywords were added.
12.3(14)T	This command was modified. New output relating to Skinny Client Control Protocol (SCCP), SCCP Telephony Control Application (STCAPP), and modem pass-through traffic was added.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record and command output was enhanced to display modem relay physical layer and error correction protocols.
12.4(4)T	This command was modified. The **long-dur-call** keyword was added.
12.4(11)XW	This command was modified. The **stats** keyword was added.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

Use this command to display the contents of the active voice call table. This command displays information about call times, dial peers, connections, and quality of service, and other status and statistical information for voice calls currently connected through the router.

Before you can query the echo state, you need to know the hexadecimal ID. To find the hexadecimal ID, enter the **show call active voice brief** command or use the **show voice call status** command.

When the extended EC is present, the **show call active voice** command displays the contents of the Ditech EC_CHAN_CTRL structure. Table 54 contains names and descriptions of the fields in the EC_CHAN_CTRL structure. Table 54 also provides a listing of the information types associated with this command.

Table 54 EC_CHAN_CTRL Field Descriptions

Symbol	Field	Description
BYP0	Channel bypass	• 1 = Transparent bypass; EC is disabled. • 0 = Cancel; EC is enabled.
TAIL3	Max tail	• 0 = 24 milliseconds. • 1 = 32 milliseconds. • 2 = 48 milliseconds. • 3 = 64 milliseconds. **Note** This field should be set just greater than the anticipated worst round-trip tail delay.
REC3	Residual echo control	• 0 = Cancel only; echo is the result of linear processing; no nonlinear processing is applied. • 1 = Suppress residual; residual echo is zeroed; simple nonlinear processing is applied (you might experience “dead air” when talking). • 2 = Reserved. • 3 = Generate comfort noise (default).
FRZ0	h-register hold	1 = Freezes h-register; used for testing.
HZ0	h-register clear	Sending the channel command with this bit set clears the h-register.
TD3	Modem tone disable	• 0 = Ignore 2100 Hz modem answer tone. • 1 = G.164 mode (bypass canceller if 2100 Hz tone). • 2 = R. • 3 = G.165 mode (bypass canceller for phase reversing tone only).
ERL0	Echo return loss	• 0 = 6 decibel (dB). • 1 = 3 dB. • 2 = 0 dB. • 3 = R. Worst echo return loss (ERL) situation in which canceller still works.
HLC1	High level compensation	• 0 = No attenuation. • 1 = 6 dB if clipped. On loud circuits, the received direction can be attenuated 6 dB if clipping is observed.
R0	Reserved	Must be set to 0 to ensure compatibility with future releases.

Use the **show call active voice redirect tbct** command to monitor any active calls that implement RTPvt or TBCT.

When a call is no longer active, its record is stored. You can display the record by using the **show call history voice** command.

Examples

The following is sample output from the **show call active voice** command for modem relay traffic:

```
Router# show call active voice

Modem Relay Local Rx Speed=0 bps
Modem Relay Local Tx Speed=0 bps
Modem Relay Remote Rx Speed=0 bps
Modem Relay Remote Tx Speed=0 bps
Modem Relay Phy Layer Protocol=v34
Modem Relay Ec Layer Protocol=v14
SPRTInfoFramesReceived=0
SPRTInfoTFramesSent=0
SPRTInfoTFramesResent=0
SPRTXidFramesReceived=0
SPRTXidFramesSent=0
SPRTTotalInfoBytesReceived=0
SPRTTotalInfoBytesSent=0
SPRTPacketDrops=0
```

Table 55 describes the significant fields shown in the display.

Table 55 show show call active voice Field Descriptions

Field	Description
Modem Relay Local Rx Speed	Download speed, in bits per second, of the local modem relay.
Modem Relay Local Tx Speed	Upload speed of the local modem relay.
Modem Relay Remote Rx Speed	Download speed of the remote modem relay.
Modem Relay Remote Tx Speed	Upload speed of the remote modem relay.
Modem Relay Phy Layer Protocol	Physical protocol of the modem relay.
Modem Relay Ec Layer Protocol	EC layer protocol of the modem relay.
SPRTInfoFramesReceived	Total number of simple packet relay transport (SPRT) protocol frames received.
SPRTInfoTFramesSent	Total number of SPRT frames sent.
SPRTInfoTFramesResent	Total number of SPRT frames sent again.
SPRTXidFramesReceived	Total number of SPRTS ID frames received.
SPRTXidFramesSent	Total number of SPRTS ID frames sent.
SPRTTotalInfoBytesReceived	Total number of SPRT bytes received.
SPRTTotalInfoBytesSent	Total number of SPRT bytes sent.
SPRTPacketDrops	Total number of SPRT packets dropped.

The following is sample output from the **show call active voice** command:

```
Router# show call active voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
```

```
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

 GENERIC:
SetupTime=1072620 ms
Index=1
PeerAddress=9193927582
PeerSubAddress=
PeerId=8
PeerIfIndex=19
LogicalIfIndex=0
ConnectTime=1078940 ms
CallDuration=00:00:51 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=1490
TransmitBytes=0
ReceivePackets=2839
ReceiveBytes=56780
VOIP:
ConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=1
RemoteIPAddress=10.44.44.44
RemoteUDPPort=17096
RemoteSignallingIPAddress=10.44.44.44
RemoteSignallingPort=56434
RemoteMediaIPAddress=10.44.44.44
RemoteMediaPort=17096
RoundTripDelay=6 ms
SelectedQoS=best-effort
tx_DtmfRelay=h245-signal
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=54160
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=60 ms
TxPakNumber=1490
TxSignalPak=0
TxComfortNoisePak=1
TxDuration=54240
TxVoiceDuration=29790
RxPakNumber=2711
RxSignalPak=0
RxDuration=0
TxVoiceDuration=54210
VoiceRxDuration=54160
```

```
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=60
PlayDelayMin=60
PlayDelayMax=70
PlayDelayClockOffset=212491899
PlayDelayJitter=0 ms
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=10
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-57
InSignalLevel=-51
LevelTxPowerMean=0
LevelRxPowerMean=-510
LevelBgNoise=0
ERLLevel=16
ACOMLevel=16
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=60 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

 GENERIC:
SetupTime=1072760 ms
Index=1
PeerAddress=93615494
PeerSubAddress=
PeerId=9
```

```
PeerIfIndex=18
LogicalIfIndex=4
ConnectTime=1078940 ms
CallDuration=00:00:53 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2953
TransmitBytes=82684
ReceivePackets=1490
ReceiveBytes=29781
TELE:
ConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=2
Port=3/0/0 (1)
BearerChannel=3/0/0.2
TxDuration=59080 ms
VoiceTxDuration=29790 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-54
ACOMLevel=16
OutSignalLevel=-57
InSignalLevel=-51
InfoActivity=1
ERLLevel=16
EchoCancellerMaxReflector=8
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
AlertTimepoint=1073340 ms
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwOutpulsedCalledNumber=93615494
GwOutpulsedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
GwOutpulsedCallingNumber=9193927582
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
DSPIdentifier=3/1:1
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Table 54 on page 1848 and Table 53 describe the significant fields shown in the display, in alphabetical order.

Table 56 show call active voice Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) delay during this call, in ms.

Table 56 show call active voice Field Descriptions

Field	Description
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.

Table 56 show call active voice Field Descriptions

Field	Description
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active voice** command for voice traffic over call-agent controlled call legs. Note that call legs for SCCP telephony endpoints, that is, phones controlled by STCAPP, are displayed under the "Call agent controlled call-legs" field ("SCCP call-legs" displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing).

```
Router# show call active voice

Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4

 GENERIC:
SetupTime=1557650 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=10
ConnectTime=1562040 ms
CallDuration=00:01:01 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=3101
TransmitBytes=519564
ReceivePackets=3094
ReceiveBytes=494572
TELE:
ConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
IncomingConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
CallID=25
Port=3/0/0 (25)
BearerChannel=3/0/0.1
TxDuration=59670 ms
VoiceTxDuration=59670 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
```

```
NoiseLevel=-12
ACOMLevel=22
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=22
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
DSPIdentifier=1/1:1

 GENERIC:
SetupTime=1559430 ms
Index=1
PeerAddress=7702
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=11
ConnectTime=1562020 ms
CallDuration=00:01:03 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3151
TransmitBytes=528900
ReceivePackets=3158
ReceiveBytes=503876
TELE:
ConnectionId=[0x0 0x0 0x0 0x0]
IncomingConnectionId=[0x0 0x0 0x0 0x0]
CallID=26
Port=3/0/0 (26)
BearerChannel=3/0/0.2
TxDuration=60815 ms
VoiceTxDuration=60815 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-12
ACOMLevel=28
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=28
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
```

```
AlertTimepoint=1559430 ms
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=7701
TranslatedCallingOctet=0x0
TranslatedCalledNumber=7702
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwOutpulsedCalledNumber=7702
GwOutpulsedCalledOctet3=0x0
GwOutpulsedCallingNumber=7701
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
DSPIdentifier=1/1:2

 GENERIC:
SetupTime=1562040 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3215
TransmitBytes=512996
ReceivePackets=3208
ReceiveBytes=512812
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=27
RemoteIPAddress=10.10.0.0
RemoteUDPPort=17718
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=17718
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=60640
GapFillWithSilence=0 ms
```

```
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
LoWaterPlayoutDelay=105 ms
TxPakNumber=3040
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=60815
TxVoiceDuration=60815
RxPakNumber=3035
RxSignalPak=0
RxDuration=0
TxVoiceDuration=60690
VoiceRxDuration=60640
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=-1662143961
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-115
LevelBgNoise=0
ERLLevel=28
ACOMLevel=28
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
```

```
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

 GENERIC:
SetupTime=1562040 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3380
TransmitBytes=540332
ReceivePackets=3386
ReceiveBytes=540356
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=28
RemoteIPAddress=10.0.0.0
RemoteUDPPort=18630
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=18630
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=63120
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
```

```
LoWaterPlayoutDelay=105 ms
TxPakNumber=3158
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=63165
TxVoiceDuration=63165
RxPakNumber=3164
RxSignalPak=0
RxDuration=0
TxVoiceDuration=63165
VoiceRxDuration=63120
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=957554296
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-114
LevelBgNoise=0
ERLLevel=22
ACOMLevel=22
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
```

```
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4
```

Table 54 on page 1848 and Table 53 on page 1842 describe the significant fields shown in the display, in alphabetical order.

The following is sample output from the **show call active voice** command to indicate if Service Advertisement Framework (SAF) is being used:

```
Router# show call active voice

Total call-legs: 2
GENERIC:
SetupTime=1971780 ms
Index=1
PeerAddress=6046692010
PeerSubAddress=
PeerId=20003
PeerIfIndex=17
.
.
.
VOIP:
SessionProtocol=sipv2
ProtocolCallId=7A9E7D9A-EAD311DC-8036BCC4-6EEE85D6@1.5.6.12
SessionTarget=1.5.6.10
SafEnabled=TRUE
SafTrunkRouteId=1
SafPluginDialpeerTag=8
```

Table 54 on page 1848 and Table 58 on page 1865 describe the significant fields shown in the display. The following is sample output from the **show call active voice** command for fax-relay traffic:

```
Router# show call active voice

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

 GENERIC:
SetupTime=1049400 ms
Index=2
PeerAddress=52930
PeerSubAddress=
PeerId=82
```

```
PeerIfIndex=222
LogicalIfIndex=0
ConnectTime=105105
CallDuration=00:00:59
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=1837
TransmitBytes=29764
ReceivePackets=261
ReceiveBytes=4079
VOIP:
ConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
IncomingConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
RemoteIPAddress=10.7.95.3
RemoteUDPPort=16610
RemoteSignallingIPAddress=10.7.95.3
RemoteSignallingPort=1720
RemoteMediaIPAddress=10.7.95.3
RemoteMediaPort=16610
RoundTripDelay=13 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=ipv4:10.7.95.3
OnTimeRvPlayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=110 ms
LoWaterPlayoutDelay=70 ms
ReceiveDelay=70 ms
LostPackets=0
EarlyPackets=1
LatePackets=0
VAD = enabled
CoderTypeRate=t38
CodecBytes=40
Media Setting=flow-through
AlertTimepoint=104972
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x7F
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
```

```
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwOutpulsedCalledNumber=52930
GwOutpulsedCalledOctet3=0xE9
GwReceivedCallingNumber=555-0100
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x80
Username=
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

Table 54 on page 1848 and Table 58 on page 1865 describe the significant fields shown in the display.

The following is sample output from the **show call active voice brief** command:

```
Router# show call active voice brief

<ID>: <CallID> <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
long_duration_call_detected:<y/n> long duration call duration:n/a timestamp:n/a
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Total call-legs:2
1269 :7587246hs.1 +260 pid:0 Answer  active
 dur 00:07:14 tx:590/11550 rx:21721/434420
IP 172.29.248.111:17394 rtt:3ms pl:431850/0ms lost:0/0/0 dela
y:69/69/70ms g729r8

1269 :7587246hs.2 +259 pid:133001 Originate 133001 active
 dur 00:07:14 tx:21717/434340 rx:590/11550
 Tele 1/0:1 (2):tx:434350/11640/0ms g729r8 noise:-44 acom:-19
i/0:-45/-45 dBm
```

The following is an example of the **show call active voice** command using the **echo-canceller** keyword. The number 9 represents the hexadecimal ID of an active voice call.

```
Router# show call active voice echo-canceller 9

ACOM=-65  ERL=45
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=5
Ecan version = 8180
```

The following is sample output from the **show call active voice echo-canceller** command for a call with a hexadecimal ID of 10:

```
Router# show call active voice echo-canceller 10

ACOM=-15  ERL=7
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=64
```

The call ID number (which is 10 in the preceding example) changes with every new active call. When an active call is up, you must enter the **show call active voice brief** command to obtain the call ID number. The call ID must be converted to hexadecimal value if you want to use the **show call active voice echo-canceller** *x* command (*x* = call ID converted to hexadecimal value).

Table 57 shows call ID examples converted to hexadecimal values (generally incremented by 2):

Table 57 Call IDs Converted to Hex

Decimal	Hex
2	2
4	4
6	6
8	8
10	A
12	C

Alternatively, you can use the **show voice call status** command to obtain the call ID. The call ID output is already in hexadecimal values form when you use this command:

```
Router# show voice call status

CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x1        11CE 0x02407B20 1:0.1     1/1     1000       g711ulaw 2000/1000
```

The following is sample output from the **show call active voice** command using the **compact** keyword:

```
Router# show call active voice compact

<callID>   A/O FAX T<sec> Codec    type    Peer Address    IP R<ip>:<udp>
Total call-legs: 2
58 ANS     T11          g711ulaw   VOIP     Psipp 2001:.....:230A:6080
59 ORG     T11          g711ulaw   VOIP     P5000110011       10.13.37.150:6090
```

The following is sample output from the **show call active voice redirect** command using the **tbct** keyword:

```
Router# show call active voice redirect tbct

TBCT:
        Maximum no. of TBCT calls allowed:No limit
        Maximum TBCT call duration:No limit


Total number TBCT calls currently being monitored = 1

ctrl name=T1-2/0, tag=13, call-ids=(7, 8), start_time=*00:12:25.985 UTC Mon Mar 1 1993
```

Table 58 describes the significant fields shown in the display.

Table 58 show call active voice redirect Field Descriptions

Field	Description
Maximum no. of TBCT calls allowed	Maximum number of calls that can use TBCT as defined by the **tbct max calls** command.
Maximum TBCT call duration	Maximum length allowed for a TBCT call as defined by the **tbct max call-duration** command.
Total number TBCT calls currently being monitored	Total number of active TBCT calls.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
call-ids	Numbers that uniquely identify the call legs.
start_time	Time, in hours, minutes, and seconds, when the redirected call began.

Related Commands

Command	Description
show call active fax	Displays call information for fax transmissions that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice call status	Displays the call status for voice ports on the Cisco router or concentrator.
show voice port	Displays configuration information about a specific voice port.

show call application app-level

To display application-level statistics for voice applications, use the **show call application app-level** command in privileged EXEC mode.

show call application {**active** | **history**} **app-level** [**app-tag** *application-name* | **summary**]

Syntax Description

active	Displays statistics for active application instances.
history	Displays statistics for terminated application instances.
app-tag *application-name*	Name of a specific voice application. Output displays statistics for that voice application.
summary	Displays a summary for each application.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display statistics with this command, you must enable statistics collection with the **call application stats** command.
- This command displays gauges and counters that are aggregated per application. The values represent all instances of a particular voice application running on the gateway while statistics collection is enabled.
- To reset application-level counters to zero and subtract the counters from the gateway-level statistics in history, use the **clear call application stats** command. Statistic counters continue accumulating in history until you use the **clear call application stats** command or the gateway reloads.

Note Statistics for an application are automatically cleared if the application is deleted with the **no call application voice** command or its script is reloaded with the **call application voice load** command.

Examples

The following is sample output from the **show call application app-level** command using different keywords:

```
Router# show call application active app-level summary

Application level active Info:
                              Sessions
App Name                   w/ Stats   Total
session                    0          0
fax_hop_on                 0          0
clid_authen                0          0
clid_authen_collect        0          0
clid_authen_npw            0          0
```

```
clid_authen_col_npw      0          0
clid_col_npw_3           0          0
clid_col_npw_npw         0          0
Default                  0          0
lib_off_app              0          0
fax_on_vfc_onramp_app    0          0
asr                      0          0
offramp                  0          0
generic                  1          1
smtp_record              0          0
authen                   0          0
authorize                0          0
ram_record_replay        0          0

Router# show call application active app-level app-tag generic

Application level active Info:

Application Name:              generic
url:                           tftp://10.10.10.113/tftplocal/generic.vxml
Total sessions:                                  1
Sessions w/ stats:                               1
Currently connected incoming PSTN legs:          1
Currently connected outgoing PSTN legs:          0
Currently connected incoming VoIP legs:          0
Currently connected outgoing VoIP legs:          0
Placecalls in transit:                           0
Handouts in transit:                             0
Pending ASNL subscriptions:                      0
Pending ASNL unsubscriptions:                    0
Prompts playing (non-TTS):                       0
Recordings:                                      0
TTS prompts playing:                             0
```

For a description of the fields shown in the display above, see Table 38 on page 1363.

```
Router# show call application history app-level summary

Application level history Info:
                                  Sessions                      Last Reset
App Name                 Stats w/ Stats   Total      Errors     Time
session                  N     0          0          0
fax_hop_on               N     0          0          0
clid_authen              N     0          0          0
clid_authen_collect      N     0          0          0
clid_authen_npw          N     0          0          0
clid_authen_col_npw      N     0          0          0
clid_col_npw_3           N     0          0          0
clid_col_npw_npw         N     0          0          0
Default                  N     0          0          0
lib_off_app              N     0          0          0
fax_on_vfc_onramp_app    N     0          0          0
ram_record_replay        N     0          0          0
authorize                N     0          0          0
authen                   N     0          0          0
smtp_record              N     0          0          0
generic                  Y     2          2          4          *Jul  3 15:49:28
offramp                  N     0          0          0
asr                      N     0          0          0
```

Table 59 describes the fields shown in the display.

Table 59 show call application history app-level Field Descriptions

Field	Description
App Name	Name of the voice application.
Stats	Whether statistics is enabled for this application. **Note** If statistics is enabled, this field displays N until there is at least one active instance of the application.
Sessions w/ stats	Number of terminated application instances that the gauges represent.
Total	Total number of instances of the application.
Errors	Total number of errors for all instances of the application.
Last Reset Time	Time at which the statistics were last cleared with the **clear call application stats** command, or the gateway was restarted.

```
Router# show call application history app-level app-tag generic

Application level history Info:

Application name:              generic
URL:                           tftp://10.10.10.113/tftplocal/generic.vxml
Total sessions:                2
Sessions w/ stats:             2
Last reset time:               *Jul  3 15:49:28 PST
Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                          Incoming Outgoing  Incoming Outgoing
Legs setup:                               2        0         0        0
Total legs connected:                     2        0         0        0
Legs handed in:                           0        0         0        0
Legs handed in returned back:             0        0         0        0
Legs handed out:                          0        0         0        0
Legs handed out came back:                0        0         0        0
Legs disconnected normally:               2        0         0        0
Legs disconnected for user error:         0        0         0        0
Legs disconnected for system error:       0        0         0        0

 Subscriber Service - Media
                                          Play       Record     TTS
Media attempts:                           3          0          0
Media successes:                          0          0          0
Media aborts:                             0          0          0
Media failures:                           3          0          0
Total media duration (in seconds):        3          0          0

 Application Internal Service - Handoff
                                          Incoming   Outgoing
Bridged handoffs:                         0          0
Bridged handoffs returned:                0          0
Blind handoffs:                           0          0
Handoffs failed:                          x          0

 Application Internal Service - Placecall/transfer
Placecall requests:                       0
Placecall successes:                      0
Placecall failures:                       0
```

```
 Application Internal Service - Document Read-Write
                                        Read       Write
Doc requests:                           0          0
Doc successes:                          0          0
Doc failures:                           0          0

 Application Internal Service - Downloaded Script
Script parse errors:                    0

 Application Internal Service - ASNL
ASNL notifications:                     0
                                        Subscription   Unsubscription
ASNL requests:                          0              0
ASNL successes:                         0              0
ASNL failures:                          0              0

 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         1
DTMFs long pound:                       0

Subscriber Interaction - ASR
ASRs not matched:                       0
ASRs matched:                           0
ASRs no input:                          0

 Subscriber Interaction - AAA
                                        Authentication Authorization
AAA successes:                          0              1
AAA failures:                           0              0
.
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application stats	Enables statistics collection for voice applications.
call application voice event-log	Enables event logging for a specific voice application.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.

show call application gateway-level

To display gateway-level statistics for voice application instances, use the **show call application gateway-level** command in privileged EXEC mode.

show call application {**active** | **history**} **gateway-level**

Syntax Description

active	Displays statistics for active application instances.
history	Displays statistics for terminated application instances.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display statistics with this command, you must enable statistics collection with the **call application stats** command.
- This command displays gauges and counters that are aggregated per gateway. The values represent all instances of all voice applications running on the gateway while statistics collection is enabled.
- To reset application-level counters to zero and subtract the counters from the gateway-level statistics in history, use the **clear call application stats** command. Statistic counters continue accumulating in history until you use the **clear call application stats** command or the gateway reloads.

Note Statistics for an application are automatically cleared if the application is deleted with the **no call application voice** command or its script is reloaded with the **call application voice load** command.

Examples

The following is sample output from the **show call application gateway-level** command using different keywords:

```
Router# show call application active gateway-level

Gateway level statistics for active application sessions:
Sessions w/ stats:                              1
Currently connected incoming PSTN legs:         1
Currently connected outgoing PSTN legs:         0
Currently connected incoming VoIP legs:         0
Currently connected outgoing VoIP legs:         0
Placecalls in transit:                          0
Handouts in transit:                            0
Pending ASNL subscriptions:                     0
Pending ASNL unsubscriptions:                   0
Prompts playing (non-TTS):                      0
Recordings:                                     0
TTS prompts playing:                            0
```

Table 60 describes the fields shown in the display.

Table 60 show call application active gateway-level Field Descriptions

Field	Description
Sessions w/ stats	Number of active application instances that the gauges represent.
Currently connected incoming PSTN legs	Number of active call legs that are incoming from the PSTN.
Currently connected outgoing PSTN legs	Number of active call legs that are outgoing to the PSTN.
Currently connected incoming VoIP legs	Number of active call legs that are incoming from the IP network.
Currently connected outgoing VoIP legs	Number of active call legs that are outgoing to the IP network.
Placecalls in transit	Number of outgoing calls in progress for all active application instances. The value is decremented by one after the call is either set up or the setup fails.
Handouts in transit	Number of handoffs in progress for all active application instances. The value is decremented by one after the receiving application either hands back the application or rejects the handoff.
Pending ASNL subscriptions	Number of Application Subscribe Notify Layer (ASNL) subscription requests that are in progress for all active application instances.
Pending ASNL unsubscriptions	Number of ASNL unsubscription requests that are in progress for all active application instances.
Prompts playing (non-TTS)	Number of recorded prompts being played in all active application instances.
Recordings	Number of recordings being made in all active application instances.
TTS prompts playing	Number of text-to-speech (TTS) prompts playing in all active application instances.

```
Router# show call application history gateway-level

Gateway level statistics for history application sessions:
Sessions w/ stats:              2
Last reset time:                *Jul  3 15:49:28 PST
Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                          Incoming Outgoing  Incoming Outgoing
Legs setup:                               2        0         0        0
Total legs connected:                     2        0         0        0
Legs handed in:                           0        0         0        0
Legs handed in returned back:             0        0         0        0
Legs handed out:                          0        0         0        0
Legs handed out came back:                0        0         0        0
Legs disconnected normally:               2        0         0        0
Legs disconnected for user error:         0        0         0        0
```

```
Legs disconnected for system error:        0        0         0        0

 Subscriber Service - Media
                                           Play       Record     TTS
Media attempts:                            3          0          0
Media successes:                           0          0          0
Media aborts:                              0          0          0
Media failures:                            3          0          0
Total media duration (in seconds):         3          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                         0
DTMFs matched:                             0
DTMFs no input:                            1
DTMFs long pound:                          0
```

For a description of the fields shown with the **history** keyword.

Related Commands

Command	Description
call application stats	Enables statistics collection for voice applications.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application app-level	Displays application-level statistics for voice applications.
show call application session-level	Displays event logs and statistics for voice application instances.

show call application interface

To display event logs and statistics for application interfaces, use the **show call application interface** command in privileged EXEC mode.

show call application interface [**summary** | {**aaa** | **asr** | **flash** | **http** | **ram** | **rtsp** | **smtp** | **tftp** | **tts**} [**server** *server*] [**event-log** | **info** | **summary**]]

Syntax Description

summary	(Optional) Displays a short summary of all interface types or the selected interface.
aaa	Authentication, authorization, and accounting (AAA) interface type.
asr	Automatic speech recognition (ASR) interface type.
flash	Flash memory of the Cisco gateway.
http	Hypertext Transfer Protocol (HTTP) interface type.
ram	Memory of the Cisco gateway.
rtsp	Real Time Streaming Protocol (RTSP) interface type.
smtp	Simple Mail Transfer Protocol (SMTP) interface type.
tftp	Trivial File Transfer Protocol (TFTP) interface type.
tts	Text-to-speech (TTS) interface type.
server *server*	(Optional) Displays event logs or statistics for the specified server.
event-log	(Optional) Displays event logs for the selected interface type or server.
info	(Optional) Displays statistics for the selected interface type or server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you use the **server** keyword, only statistics or event logs for that server display. To display event logs or statistics with this command, you must enable statistics and event logging with the **call application interface event-log** and **call application interface stats** command, respectively. To reset statistic counters to zero and clear the event logs in history, use the **clear call application interface** command.

Examples

The following is sample output from the **show call application interface** command using different keywords:

```
Router# show call application interface summary

Aggregated statistics for http service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   3
Read successes:                  0
Read failures:                   3
```

```
Read aborts:                    0
Total bytes read:               0
Write requests:                 0
Write successes:                0
Write failures:                 0
Write aborts:                   0
Total bytes written:            0

Aggregated statistics for tts service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                  0
Read successes:                 0
Read failures:                  0
Read aborts:                    0

Aggregated statistics for asr service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                  0
Read successes:                 0
Read failures:                  0
Read aborts:                    0

Aggregated statistics for tftp service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                  3
Read successes:                 2
Read failures:                  0
Read aborts:                    1
Total bytes read:               145888

Router# show call application interface tftp summary

Aggregated statistics for tftp service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                  3
Read successes:                 2
Read failures:                  0
Read aborts:                    1
Total bytes read:               145888

Server Name          Stats Error Count            Event Log
172.19.139.145       Y     0                      Y
speech-serv          Y     0                      N

Router# show call application interface tftp

Server name:         172.19.139.145

Statistics:
Last reset time *Jul  3 16:08:13 PST
Read requests:                  1
Read successes:                 2
Read failures:                  0
Read aborts:                    1
Total bytes read:               145888

Event log:
Last reset time *Jul  3 16:08:13 PST
buf_size=50K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
172.19.139.145:1057277293:53:INFO: ID = 6549D9E0: Read requested for URL =
tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277295:54:INFO: ID = 6549D9E0: Streamed read transaction Successful URL
= tftp://172.19.139.145/audio/ch_welcome.au
```

```
172.19.139.145:1057277306:59:INFO: ID = 649A0320: Streamed read transaction Successful URL
= tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277317:65:INFO: ID = 650922A8: Read request aborted for URL =
tftp://172.19.139.145/audio/ch_welcome.au
-------------------------------------------------------------------------------

Router# show call application interface tftp event-log

Server name:         172.19.139.145

Event log:
Last reset time *Jul  3 16:08:13 PST
buf_size=50K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
172.19.139.145:1057277293:53:INFO: ID = 6549D9E0: Read requested for URL =
tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277295:54:INFO: ID = 6549D9E0: Streamed read transaction Successful URL
= tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277306:59:INFO: ID = 649A0320: Streamed read transaction Successful URL
= tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277317:65:INFO: ID = 650922A8: Read request aborted for URL =
tftp://172.19.139.145/audio/ch_welcome.au
-------------------------------------------------------------------------------

Router# show call application interface tftp info

Server name:         172.19.139.145

Statistics:
Last reset time *Jul  3 16:08:13 PST
Read requests:             3
Read successes:            2
Read failures:             0
Read aborts:               1
Total bytes read:                145888
-------------------------------------------------------------------------------
```

Table 61 describes the significant fields shown in the display.

Table 61 show call application interface Field Descriptions

Field	Description
Last reset time	Time at which the statistics were last cleared with the **clear call application interface** command, or the gateway was restarted.
Read requests	Total number of read requests from applications to this interface type.
Read successes	Number of successful read requests from applications to this interface type.
Read failures	Number of failed read requests from applications to this interface type.
Read aborts	Number of aborted read requests from applications to this interface type.
Total bytes read	Total number of bytes that the application read from this interface type.
Server name	Name of the specific server.

Table 61 show call application interface Field Descriptions

Field	Description
Stats	Whether statistics are enabled for this server.
Error Count	Total number of errors for this server.
Event Log	Whether event logging is enabled for this server.

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface stats	Enables statistics collection for application interfaces.
clear call application interface	Clears application interface statistics and event logs.

show call application services registry

To display a one-line summary of all TCL IVR 2.0 application sessions that have registered as a service, use the **show call application services registry** command in user EXEC or privileged EXEC mode.

show call application services registry

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- The services registry is a database that keeps track of every TCL IVR 2.0 application instance that registers as a service. Other TCL applications can then find and communicate with any registered application.
- A TCL session is not registered as a service through a Cisco IOS command. A running instance of a TCL IVR 2.0 application registers itself as a service with the TCL service register command. For information about the service register command, refer to the *TCL IVR API Version 2.0 Programmer's Guide*.

Examples

The following is sample output for this command:

```
Router# show call application services registry

There are 1 Registered Services
  Service Name         Session ID  Session Name
  data_service                  4  s1
```

Table 62 describes significant fields in the display.

Table 62 show call application services registry Field Descriptions

Field	Description
Service Name	Name specified by the TCL service register command.
Session ID	ID of the session that registered as this service. You can use this ID in the **show call application sessions id** command to view details about this session.
Session Name	Name configured by the **call application session start** command, if the session was started on the gateway rather than by an incoming call.

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a TCL application from global configuration mode.
call application session start (privileged EXEC)	Starts a new instance (session) of a TCL application from privileged EXEC mode.
call application session stop	Stops a voice application session that is running.
show call application sessions	Displays summary or detailed information about voice application sessions.

show call application session-level

To display event logs and statistics for individual voice application instances, use the **show call application session-level** command in privileged EXEC mode.

show call application {**active** | **history**} **session-level** [**summary** | [**app-tag** *application-name* | **last** [*number*] | **session-id** *session-id*] [**event-log** | **info**]]

Syntax Description

active	Displays event logs or statistics for active application instances.
history	Displays event logs or statistics for inactive application instances in the history table.
summary	Displays a summary of each application instance.
app-tag *application-name*	Name of a specific voice application. Output displays event logs or statistics for that voice application.
last	(Optional) Displays event logs or statistics for the most recent instance.
number	(Optional) Displays event logs or statistics for this number of most recent previous instances.
session-id *session-id*	Identifies a specific application instance. Output displays event logs or statistics for that instance.
event-log	(Optional) Displays event logs for application instances.
info	(Optional) Displays statistics for application instances.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display event logs or statistics with this command, you must enable event logging and statistics with the **call application event-log** and **call application stats** command, respectively.
- This command displays gauges and counters that are aggregated per application instance. The values represent an individual instance running on the gateway while statistics collection is enabled.
- The number of records that are included when using the **history** keyword depends on the settings of the **call application history session max-records** and **call application history session retain-timer** commands.

Examples

The following is sample output from the **show call application session-level** command using different keywords and arguments:

```
Router# show call application active session-level summary

SID  Application Name       Stat Err Cnt    Log Start Time
5    generic                Y    6          Y   *Jul  3 15:19:4
6    generic                Y    3          Y   *Jul  3 15:19:5

Router# show call application active session-level last

Session Info:
Session id:          6
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:19:53 PST

Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                          Incoming Outgoing  Incoming Outgoing
Legs setup:                               1        0         0        0
Total legs connected:                     1        0         0        0
Legs currently connected:                 1        0         0        0
Legs handed in:                           0        0         0        0
Legs handed in returned back:             0        0         0        0
Legs handed out:                          0        0         0        0
Legs handed out came back:                0        0         0        0
Legs disconnected normally:               0        0         0        0
Legs disconnected for user error:         0        0         0        0
Legs disconnected for system error:       0        0         0        0

 Subscriber Service - Media
                                          Play       Record     TTS
Media attempts:                           4          0          0
Media actives:                            0          0          0
Media successes:                          0          0          0
Media aborts:                             0          0          0
Media failures:                           4          0          0
Total media duration (in seconds):        0          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                        0
DTMFs matched:                            0
DTMFs no input:                           3
DTMFs long pound:                         0

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
6:1057274393:472:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
6:1057274393:473:INFO: Incoming Telephony call received, LegID = 10
6:1057274393:474:INFO: LegID = 10: Calling = 4084644753, called = 52927, dial peer = 1
6:1057274393:475:INFO: LegID = 10: Leg State = LEG_INCCONNECTED
6:1057274393:478:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
6:1057274408:517:INFO: Script received event = "error.badfetch"

Router# show call application active session-level info

Session Info:
Session id:          5
```

```
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:19:44 PST

Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0

 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         9          0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         9          0          0
Total media duration (in seconds):      0          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         8
DTMFs long pound:                       0

Session Info:
Session id:          6
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:19:53 PST

Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             3        0         0        0
Total legs connected:                   3        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0

 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         7          0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         7          0          0
```

```
Media duration (in seconds):                0           0           0

 Application Internal Service - Handoff
                                            Incoming    Outgoing
Bridged handoffs:                           0           0
Bridged handoffs returned:                  0           0
Blind handoffs:                             0           0
Handoffs in transit:                        x           0
Handoffs failed:                            x           0

 Application Internal Service - Placecall/transfer
Placecall requests:                         0
Placecall successes:                        0
Placecall failures:                         0
Placecalls in transit:                      0

 Application Internal Service - Document Read-Write
                                            Read        Write
Doc requests:                               0           0
Doc successes:                              0           0
Doc failures:                               0           0

 Application Internal Service - Downloaded Script
Script parse errors:                        0

 Application Internal Service - ASNL
ASNL notifications:                         0
                                            Subscription    Unsubscription
ASNL requests:                              0               0
ASNL successes:                             0               0
ASNL pendings:                              0               0
ASNL failures:                              0               0

 Subscriber Interaction - DTMF
DTMFs not matched:                          0
DTMFs matched:                              0
DTMFs no input:                             6
DTMFs long pound:                           0

 Subscriber Interaction - ASR
ASRs not matched:                           0
ASRs matched:                               0
ASRs no input:                              0

 Subscriber Interaction - AAA
                                            Authentication  Authorization
AAA successes:                              0               0
AAA failures:                               0               0

Router# show call application active session-level event-log

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
5:1057274384:454:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
5:1057274384:455:INFO: Incoming Telephony call received, LegID = D
5:1057274384:456:INFO: LegID = D: Calling = 4085550198, called = 52927, dial peer = 1
5:1057274384:457:INFO: LegID = D: Leg State = LEG_INCCONNECTED
5:1057274384:460:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
5:1057274384:462:ERR : Prompt play setup failure.
5:1057274384:463:INFO: Script received event = "error.badfetch"
5:1057274389:464:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057274389:465:INFO: Script received event = "noinput"
```

```
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
6:1057274393:472:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
6:1057274393:473:INFO: Incoming Telephony call received, LegID = 10
6:1057274393:474:INFO: LegID = 10: Calling = 4084644753, called = 52927, dial peer = 1
6:1057274393:475:INFO: LegID = 10: Leg State = LEG_INCCONNECTED
6:1057274393:478:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
6:1057274393:480:ERR : Prompt play setup failure.
6:1057274393:481:INFO: Script received event = "error.badfetch"
6:1057274398:488:INFO: Timed out waiting for user DTMF digits, no user input.
6:1057274398:489:INFO: Script received event = "noinput"
6:1057274398:490:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au

Router# show call application active session-level app-tag generic

Session Info:
Session id:          5
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:19:44 PST

Statistics:
 Subscriber Service - Call
                                              PSTN                VOIP
                                       Incoming Outgoing  Incoming Outgoing
Legs setup:                            1        0         0        0
Total legs connected:                  1        0         0        0
Legs currently connected:              1        0         0        0
Legs handed in:                        0        0         0        0
Legs handed in returned back:          0        0         0        0
Legs handed out:                       0        0         0        0
Legs handed out came back:             0        0         0        0
Legs disconnected normally:            0        0         0        0
Legs disconnected for user error:      0        0         0        0
Legs disconnected for system error:    0        0         0        0

 Subscriber Service - Media
                                       Play       Record     TTS
Media attempts:                        16         0          0
Media actives:                         0          0          0
Media successes:                       0          0          0
Media aborts:                          0          0          0
Media failures:                        17         0          0
Total media duration (in seconds):     0          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                     0
DTMFs matched:                         0
DTMFs no input:                        16
DTMFs long pound:                      0

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
5:1057274384:454:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
5:1057274384:455:INFO: Incoming Telephony call received, LegID = D
5:1057274384:456:INFO: LegID = D: Calling = 4085550198, called = 52927, dial peer = 1
5:1057274384:457:INFO: LegID = D: Leg State = LEG_INCCONNECTED
5:1057274384:460:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
```

```
5:1057274384:462:ERR : Prompt play setup failure.
5:1057274384:463:INFO: Script received event = "error.badfetch"
5:1057274389:464:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057274389:465:INFO: Script received event = "noinput"
5:1057274389:466:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au

Router# show call application active session-level session-id 7

Session Info:
Session id:          7
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:21:26 PST

Statistics:
 Subscriber Service - Call
                                              PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0

 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         3          0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         3          0          0
Total media duration (in seconds):      0          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         2
DTMFs long pound:                       0

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
7:1057274486:662:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
7:1057274486:663:INFO: Incoming Telephony call received, LegID = 13
7:1057274486:664:INFO: LegID = 13: Calling = 4085550198, called = 52927, dial peer = 1
7:1057274486:665:INFO: LegID = 13: Leg State = LEG_INCCONNECTED
7:1057274486:668:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au

Router# show call application history session-level summary

SID  Application Name       Stat Err Cnt    Log Stop Time       Duration
1    generic                Y    3          Y   *Jul  3 15:49:2 00:00:11
2    generic                Y    1          Y   *Jul  3 15:49:3 00:00:03

Router# show call application history session-level last

Session Info:
```

```
Session id:          2
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:49:29 PST
Stop time:           *Jul  3 15:49:33 PST

Statistics:
 Subscriber Service - Call
                                              PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             1        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0

 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         1          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         1          0          0
Total media duration (in seconds):      0          0          0

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
2:1057276169:28:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
2:1057276169:29:INFO: Incoming Telephony call received, LegID = 4
2:1057276169:30:INFO: LegID = 4: Calling = 4085550198, called = 52927, dial peer = 1
2:1057276169:31:INFO: LegID = 4: Leg State = LEG_INCCONNECTED
2:1057276169:34:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
2:1057276169:36:ERR : Prompt play setup failure.
2:1057276169:37:INFO: Script received event = "error.badfetch"
2:1057276173:39:INFO: Script received event = "telephone.disconnect.hangup"
2:1057276173:40:INFO: LegID = 4: Call disconnected, cause = normal call clearing (16)
2:1057276173:43:INFO: Session done, terminating cause =

Router# show call application history session-level event-log

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
1:1057276157:3:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
1:1057276157:4:INFO: Incoming Telephony call received, LegID = 1
1:1057276157:5:INFO: LegID = 1: Calling = 4085550198, called = 52927, dial peer = 1
1:1057276157:6:INFO: LegID = 1: Leg State = LEG_INCCONNECTED
1:1057276157:9:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
1:1057276160:12:ERR : Prompt play setup failure.
1:1057276160:13:INFO: Script received event = "error.badfetch"
1:1057276165:14:INFO: Timed out waiting for user DTMF digits, no user input.
1:1057276165:15:INFO: Script received event = "noinput"
1:1057276165:16:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
1:1057276165:18:ERR : Prompt play setup failure.
1:1057276165:19:INFO: Script received event = "error.badfetch"
1:1057276168:21:INFO: Script received event = "telephone.disconnect.hangup"
1:1057276168:22:INFO: LegID = 1: Call disconnected, cause = normal call clearing (16)
```

```
1:1057276168:25:INFO: Session done, terminating cause =

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
2:1057276169:28:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/master/generic.vxml
2:1057276169:29:INFO: Incoming Telephony call received, LegID = 4
2:1057276169:30:INFO: LegID = 4: Calling = 4085550198, called = 52927, dial peer = 1
2:1057276169:31:INFO: LegID = 4: Leg State = LEG_INCCONNECTED
2:1057276169:34:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
2:1057276169:36:ERR : Prompt play setup failure.
2:1057276169:37:INFO: Script received event = "error.badfetch"
2:1057276173:39:INFO: Script received event = "telephone.disconnect.hangup"
2:1057276173:40:INFO: LegID = 4: Call disconnected, cause = normal call clearing (16)
2:1057276173:43:INFO: Session done, terminating cause =

Router# show call application history session-level info

Session Info:
Session id:          1
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:49:17 PST
Stop time:           *Jul  3 15:49:28 PST

Statistics:
 Subscriber Service - Call
                                              PSTN              VOIP
                                     Incoming Outgoing  Incoming Outgoing
Legs setup:                          1        0         0        0
Total legs connected:                1        0         0        0
Legs handed in:                      0        0         0        0
Legs handed in returned back:        0        0         0        0
Legs handed out:                     0        0         0        0
Legs handed out came back:           0        0         0        0
Legs disconnected normally:          1        0         0        0
Legs disconnected for user error:    0        0         0        0
Legs disconnected for system error:  0        0         0        0

 Subscriber Service - Media
                                     Play       Record     TTS
Media attempts:                      2          0          0
Media successes:                     0          0          0
Media aborts:                        0          0          0
Media failures:                      2          0          0
Total media duration (in seconds):   3          0          0

 Subscriber Interaction - DTMF
DTMFs not matched:                   0
DTMFs matched:                       0
DTMFs no input:                      1
DTMFs long pound:                    0

Session Info:
Session id:          2
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/master/generic.vxml
Start time:          *Jul  3 15:49:29 PST
Stop time:           *Jul  3 15:49:33 PST

Statistics:
```

```
 Subscriber Service - Call
                                                PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             1        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0

 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         1          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         1          0          0
Total media duration (in seconds):      0          0          0
```

Table 63 describes significant fields in the displays.

Note These fields display for the **show call application session-level**, **show call application app-level**, and **show call application gateway-level** commands. At the session level, the fields apply to a single application instance. At the application level, the fields apply to all instances of an application. At the gateway level, the fields apply to all instances of all applications.

Table 63 show call application active session-level info Field Descriptions

Field	Description
Session id	Session ID assigned to the instance when it became active.
Session name	Name of the session defined with the **call application session start** command.
Application name	Name of the application defined with the **call application voice** command.
Application URL	Location of the application script defined with the **call application voice** command.
Start time	Time at which the session started.
Subscriber Service — Call	
Legs setup	Number of calls setup (indications and requests) by an application instance.
Total legs connected	Number of calls connected by an application instance.
Legs currently connected	Number of calls currently connected by an application instance at any moment.
Legs handed in	Number of call legs received as an incoming handoff from another application.
Legs handed in returned back	Number of call legs received as an incoming handoff from another application that were returned to the other application.

Table 63 show call application active session-level info Field Descriptions (continued)

Field	Description
Legs handed out	Number of call legs handed off to another application.
Legs handed out came back	Number of call legs handed off to another application that were returned by the other application.
Legs disconnected normally	Number of incoming and outgoing calls disconnected for normal causes.
Legs disconnected for user error	Number of incoming calls disconnected for call failure reasons, such as no answer or busy.
Legs disconnected for system error	Number of incoming calls disconnected for system failure reasons, such as no resources.
Subscriber Service — Media	
Media attempts	Number of prompt playouts, recordings, and text-to-speech (TTS) attempts on call legs in this application instance.
Media actives,	Number of prompt playouts, recordings, and TTS prompts currently active on call legs in an application instance.
Media successes	Number of prompt playouts, recordings, and TTS prompts that were successful on call legs in an application instance.
Media aborts	Number of prompt playouts, recordings, and TTS prompts that were aborted by the caller on call legs in an application instance.
Media failures	Number of prompt playouts, recording, and TTS attempts that failed on call legs in an application instance.
Total media duration	Total duration, in seconds, of prompt playing, recording, or TTS.
Application Internal Service — Handoff	
Bridged handoffs, incoming	Number of handoffs received with callback (bridged transfers) in an application instance.
Bridged handoffs, outgoing	Number of handoffs placed with callback (bridged transfers) by an application instance.
Bridged handoffs returned, incoming	Number of incoming bridged handoffs that were returned by an application instance.
Bridged handoffs returned, outgoing	Number of outgoing bridged handoffs that were returned to an application instance.
Blind handoffs, incoming	Number of handoffs received with no callback (blind transfers) in an application instance.
Blind handoffs, outgoing	Number of handoffs placed with no callback (blind transfers) by an application instance.
Handoffs in transit[1]	Number of handoffs in progress for an application instance. The value is decremented by one after the receiving application either hands back the application or rejects the handoff.
Handoffs failed	Number of handoffs that failed (bridged and blind) in an application instance.
Application Internal Service — Placecall/transfer	

Table 63 show call application active session-level info Field Descriptions (continued)

Field	Description
Placecall requests	Number of outgoing call setup requests made by an application instance.
Placecall successes	Number of outgoing calls placed by an application instance.
Placecall failures	Number of outgoing call setup requests that failed for an application instance.
Placecalls in transit[1]	Number of outgoing calls in progress for an application. The value is decremented by one after the call is either set up or the setup fails.
Application Internal Service — Document Read-Write	
Doc requests	Number of document fetch and submit requests.
Doc successes	Number of successful document fetches and submits.
Doc failures	Number of document fetch and submit failures.
Application Internal Service — Downloaded Script	
Script parse errors	Number of semantic errors seen by an application instance.
Application Internal Service — ASNL	
ASNL notifications	Number of Application Subscribe Notify Layer (ASNL) notifications received from servers.
ASNL requests	Number of subscribe or unsubscribe requests made by an application instance.
ASNL successes	Number of subscribe or unsubscribe requests that succeeded for an application instance.
ANSL failures	Number of subscribe or unsubscribe requests that failed for an application instance.
Subscriber Interaction -— DTMF	
DTMFs not matched	Number of DTMF patterns input by a caller that were not matched in an application instance.
DTMFs matched	Number of DTMF patterns input by a caller that were matched in an application instance.
DTMFs no input	Number of “no input” notifications received (includes DTMF timeouts).
DTMFs long pound	Number of long-pound interrupts from a caller seen by an application instance.
Subscriber Interaction — ASR	
ASR not matched	Number of automatic speech recognition (ASR) phrases from a caller that were not matched in an application instance.
ASR matched	Number of automatic speech recognition (ASR) phrases from a caller that were matched in an application instance.
ASR no inputs	Number of “no input” notifications received from ASR servers.
Subscriber Interaction — AAA Authentication	
AAA authentication successes	Number of AAA authentication successes.

Table 63 show call application active session-level info Field Descriptions (continued)

Field	Description
AAA authentication failures	Number of AAA authentication failures because of invalid passwords.
Subscriber Interaction — AAA Authorizations	
AAA authorization successes	Number of AAA authorization successes.
AAA authorization failures	Number of AAA authorization failures.

1. When this gauge is greater than zero, the application instance might stop processing the script and the counters and gauges may appear to freeze. When the handoff or the placecall operation is finished and control is returned to the application instance, the counters and gauges are updated.

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application history session max-records	Sets the maximum number of application instance records saved in history.
call application history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
call application stats	Enables statistics collection for voice applications.
call application voice event-log	Enables event logging for a specific voice application.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.

show call application sessions

To display summary or detailed information about all running or stopped voice application sessions, use the **show call application sessions** command in user EXEC or privileged EXEC mode.

show call application sessions [**callid** *call-id* | **id** *session-id* | **name** *instance-name*]

Syntax Description

callid *call-id*	(Optional) Call-leg ID of an active call that is being controlled by the session.
id *session-id*	(Optional) Session ID for the specific application instance.
name *instance-name*	(Optional) Name assigned to the instance with the **call application session start** command.

Command Default No default behavior or values

Command Modes User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- A specific application session is identified by one of three different methods: call ID, session ID, or instance name.
- If a specific session is identified by a **callid**, **id**, or **name** keyword, this command displays information about that specific session only. If you do not use a keyword, this command displays a one-line summary of all sessions, not just those sessions that are started by the **call application session start** command.
- This command lists all running TCL IVR 2.0 and VoiceXML application sessions and TCL sessions that are stopped. A session displays a state of "stopped" if you intentionally stop it with the **call application session stop** or **no call application session start** command, or because there is a syntax error that prevents the script from running. This is the case only if the session is started with the **call application session start** command through global configuration mode.

Note If a session is started with the **call application session start** command in privileged EXEC mode, it is not tracked by the system and is therefore not shown as stopped in the output of the **show call application sessions** command.

Examples

The following is sample output from this command:

```
Router# show call application sessions

TCL Sessions
    There are 1 active TCL sessions

     SID  Name        Called     Calling               App Name                Legs
       5  serv1                                        sample_service

VXML Sessions
    No running VXML sessions

Stopped Sessions
  Instance Name        App Name             State
  my_instance1         sample               stopped
```

Table 64 describes significant fields in the display.

Table 64 show call application sessions Field Descriptions

Field	Description
SID	Session identifier for active sessions.
Name	Session name that was configured with the **call application session start** command.
Called	Called number for active calls that are using the session.
Calling	Calling number for active calls that are using the session.
App Name	Name of the application for which the instance was created.
Legs	Any active call legs that are controlled by the session.
State	Shows “stopped” for any session that is no longer running, provided that the session is started with the **call application session start** command in global configuration mode.

The following is sample output for a session named serv1:

```
Router# show call application sessions name serv1

Session named serv1 is in the start list in state running
  It is configured to start on GW reboot
  The application it runs is sample_service
  Handle is TCL_HAND*1653710732*0*3193204
TCL Session ID B
                 App: sample_service
                 URL: tftp://dev/demo/scripts/sample_service.tcl
        Session name: serv1
      Session handle: TCL_HAND*1653710732*0*3193204
           FSM State: start_state
    ID for 'show call active voice id' display: 0
                Legs:
            Services: data_service
```

Table 65 describes significant fields in the display.

Table 65 show call application sessions name Field Descriptions

Field	Description
App	Name of the application for which the instance was created.
URL	Location of the script used for the application as specified with the **call application voice** command.
Session name	Session name that was configured with the **call application session start** command.
Session handle	Handle that is returned from the TCL mod_handle infotag. A session handle is used in a TCL script on a Cisco gateway to send messages to other sessions.
FSM State	Current state in the TCL IVR 2.0 finite-state machine, as specified with the TCL fsm setstate command in the script.
ID for 'show call active voice id' display:	Call identifier.
Legs	Any active call legs that are controlled by this session.
Services	Service name for the session if it registered as a service with the TCL service register command in the script. You can display a list of all registered services with the **show call application services registry** command.

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a TCL application from global configuration mode.
call application session start (privileged EXEC)	Starts a new instance of a TCL application from privileged EXEC mode.
call application session stop	Stops a voice application session that is running.
show call application services registry	Displays a one-line summary of all registered services.

show call application voice

To display information about voice applications, use the **show call application voice** command in EXEC mode.

show call application voice [*name* | **summary**]

Syntax Description

name	(Optional) Name of the desired voice application. Output displays information about that application.
summary	(Optional) Output displays a one-line summary of each voice application.

Command Default

If both the *name* argument and **summary** keyword are omitted, command output displays detailed information about all interactive voice response (IVR) applications.

Command Modes

EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, Cisco 3745, and Cisco 7200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.3(14)T	New output was added relating to the SCCP Telephony Control Application (STCAPP).

Usage Guidelines

The **show call application voice** command displays a detailed description of each configured application.

If the name of a specific application is entered, the command displays detailed information about only that application.

If the **summary** keyword is entered, the command displays a one-line summary about each application.

If STCAPP is enabled, the **summary** command displays STCAPP as an available call application.

If an asterisk is displayed next to the application name when the **summary** keyword is used, the application is configured, but not running. Normally this is because the application was not successfully loaded, for example:

```
name                 description
*vapptest2           flash:helloworld.vxml
```

TCL scripts and VoiceXML documents can be stored in any of the following locations: TFTP, FTP, or HTTP servers; Flash memory of the gateway; or the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations and on RTSP servers.

Examples

The following example shows the output for the session Toolkit Command Language (TCL) script:

```
Router# show call application voice session

Application session
    The script is compiled into the image
    It has 0 calls active.
    Interpreted by infrastructure version 2.0

The TCL Script is:
------------------
# app_session.tcl
#---------------------------------
# August 1999, Saravanan Shanmugham
#
# Copyright (c) 1998, 1999, 2000, 2001 by cisco Systems, Inc.
# All rights reserved.
#---------------------------------
#
# This tcl script mimics the default SESSION app
#
# If DID is configured, just place the call to the dnis
# Otherwise, output dial-tone and collect digits from the
# caller against the dial-plan.
#
# Then place the call. If successful, connect it up, otherwise
# the caller should hear a busy or congested signal.

# The main routine just establishes the statemachine and then exits.
# From then on the system drives the statemachine depending on the
# events it recieves and calls the appropriate tcl procedure


#---------------------------------
#   Example Script
#---------------------------------


proc init { } {
    global param

    set param(interruptPrompt) true
    set param(abortKey) *
    set param(terminationKey) #

}

proc act_Setup { } {
    global dest
    global beep
```

```
    set beep 0

    if { [infotag get leg_isdid] } {
        set dest [infotag get leg_dnis]
        leg proceeding leg_incoming
        leg setup $dest callInfo leg_incoming
        fsm setstate PLACECALL
    } else {
        leg setupack leg_incoming
        playtone leg_incoming tn_dial

        set param(dialPlan) true
        leg collectdigits leg_incoming param
    }


}

proc act_GotDest { } {
    global dest

    set status [infotag get evt_status]

    if {  $status == "cd_004" } {
        set dest [infotag get evt_dcdigits]
        leg proceeding leg_incoming
        leg setup $dest callInfo leg_incoming

    } else {
        puts "\nCall [infotag get con_all] got event $status collecting destina"
        call close
    }
}


proc act_CallSetupDone { } {
    global beep

    set status [infotag get evt_status]

    if { $status == "ls_000"} {

        set  creditTimeLeft [infotag get leg_settlement_time leg_all]

        if { ($creditTimeLeft == "unlimited") ||
             ($creditTimeLeft == "uninitialized") } {
            puts "\n Unlimited Time"
        } else {
            # start the timer for ...
            if { $creditTimeLeft < 10 } {
                set beep 1
                set delay $creditTimeLeft
            } else {
                set delay [expr $creditTimeLeft - 10]
            }
            timer start leg_timer $delay leg_incoming
        }
    } else {
        puts "Call [infotag get con_all] got event $status collecting destinati"
        call close
    }
}
```

```
proc act_Timer { } {
    global beep
    global incoming
    global outgoing

    set incoming [infotag get leg_incoming]
    set outgoing [infotag get leg_outgoing]

    if { $beep == 0 } {
        #insert a beep ...to the caller
        connection destroy con_all
        set beep 1
    } else {
        connection destroy con_all
        fsm setstate LASTWARN
    }
}

proc act_LastWarn { } {
    media play leg_incoming flash:out_of_time.au
}

proc act_Destroy { } {
    media play leg_incoming flash:beep.au
}

proc act_Beeped { } {
    global incoming
    global outgoing

    connection create $incoming $outgoing
}

proc act_ConnectedAgain { } {
    timer start leg_timer 10 leg_incoming
}

proc act_Ignore { } {
# Dummy
    puts "Event Capture"
}

proc act_Cleanup { } {
    call close
}

init

#----------------------------------
#   State Machine
#------------------
  set fsm(any_state,ev_disconnected)  "act_Cleanup              same_state"

  set fsm(CALL_INIT,ev_setup_indication) "act_Setup            GETDEST"

  set fsm(GETDEST,ev_collectdigits_done)  "act_GotDest          PLACECALL"

  set fsm(PLACECALL,ev_setup_done)    "act_CallSetupDone    CALLACTIVE"


  set fsm(CALLACTIVE,ev_leg_timer)    "act_Timer            INSERTBEEP"
  set fsm(INSERTBEEP,ev_destroy_done) "act_Destroy          same_state"
  set fsm(INSERTBEEP,ev_media_done)   "act_Beeped           same_state"
  set fsm(INSERTBEEP,ev_create_done)    "act_ConnectedAgain   CALLACTIVE"
```

```
  set fsm(LASTWARN,ev_destroy_done)     "act_LastWarn        CALLDISCONNECT"

  set fsm(CALLACTIVE,ev_disconnected)   "act_Cleanup         CALLDISCONNECT"
  set fsm(CALLDISCONNECT,ev_disconnected)   "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_media_done)     "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_disconnect_done) "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_leg_timer)      "act_Cleanup         same_state"

  fsm define fsm CALL_INIT
```

The following is sample output for the **summary** keyword:

```
Router# show call application voice summary

name                 description

session              Basic app to do DID, or supply dialtone.
fax_hop_on           Script to talk to a fax redialer
clid_authen          Authenticate with (ani, dnis)
clid_authen_collect  Authenticate with (ani, dnis), collect if that fails
clid_authen_npw      Authenticate with (ani, NULL)
clid_authen_col_npw  Authenticate with (ani, NULL), collect if that fails
clid_col_npw_3       Authenticate with (ani, NULL), and 3 tries collecting
clid_col_npw_npw     Authenticate with (ani, NULL) and 3 tries without pw
DEFAULT              Default system session application
lib_off_app          Libretto Offramp

TCL Script Version 2.0 supported.
TCL Script Version 1.1 supported.
Voice Browser Version 2.0 for VoiceXML 1.0 & 2.0 supported.
```

The following is sample output for the **summary** keyword when STCAPP is enabled:

```
Router# show call application voice summary

 SERVICES (standalone applications):
  name                      type            description

  ipsla-responder           Tcl Script      builtin:app_test_rcvr_script.tcl
  clid_authen               Tcl Script      builtin:app_clid_authen_script.tcl
  clid_col_npw_npw          Tcl Script      builtin:app_clid_col_npw_npw_script.tcl
  DEFAULT                   C Script        builtin:Session_Service.C
  CTAPP                     C Script        builtin:CallTreatment_Service.C
  clid_authen_col_npw       Tcl Script      builtin:app_clid_authen_col_npw_script.tcl
  fax_hop_on                Tcl Script      builtin:app_fax_hop_on_script.tcl
  ipsla-testcall            Tcl Script      builtin:app_test_place_script.tcl
  clid_authen_npw           Tcl Script      builtin:app_clid_authen_npw_script.tcl
  session                   Tcl Script      builtin:app_session_script.tcl
  clid_authen_collect       Tcl Script      builtin:app_clid_authen_collect_script.tcl
  clid_col_npw_3            Tcl Script      builtin:app_clid_col_npw_3_script.tcl
  lib_off_app               CCAPI           Libretto Offramp
  DEFAULT.C.OLD             CCAPI           Obsolete system session application
  stcapp                    CCAPI           SCCP Call Control Application
  MGCPAPP                   CCAPI           MGCP Application
```

The following is sample output for the **stcapp** keyword when the STCAPP is enabled:

```
Router# show call application voice stcapp

App Status:              Active
CCM Status:              UP
CCM Group:               2
Registration Mode:       CCM
Total Devices:           5
```

```
Total Calls in Progress: 0
Total Call Legs in Use:  0
```

The following is sample output from the show call application voice command for a VoiceXML application named vapptest1:

```
Router# show call application voice vapptest1

VXML Application vapptest1
    URL=flash:demo0.vxml
    Security not trusted
    No languages configured
    It has: 0 calls active.
          0 incoming calls
          0 calls handed off to it
          0 call transfers initiated
          0 pages loaded,  0 successful
          0 prompts played
          0 recorded messages
    Interpreted by Voice Browser Version 2.0 for VoiceXML 1.0 & 2.0.

The VXML Script is:
------------------
<?xml version="1.0"?>
<vxml version="1.0">

  <form>
        <block>
      <audio src="flash:demo0.au"/>
    </block>
  </form>
</vxml>
```

Table 66 describes the fields shown in the **show call application voice** display:

Table 66 show call application voice Field Descriptions

Field	Description
URL	Location of the document used by the application.
It has: *n* calls active.	Number of calls that are using this application.
incoming calls	Number of incoming public switched telephone network (PSTN) or IP calls that invoked this application.
calls handed off to it	Number of calls that were handed off to this application by another TCL or VoiceXML application.
call transfers initiated	Number of call transfers that were initiated by this application.
pages loaded	Number of VoiceXML pages that were loaded by the application.
successful	Number of VoiceXML pages that were completed.
prompts played	Number of audio prompts that were played by the application.
recorded messages	Number of audio recordings made by the VoiceXML application.
Interpreted by	Programming language used by the application.
The TCL or VoiceXML Script is	Content of the VoiceXML document or TCL script.

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with the application.
call application voice load	Reloads the designated TCL script or VoiceXML document.

show call fallback cache

To display the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses in cache, use the **show call fallback cache** command in EXEC mode.

show call fallback cache [*ip-address*]

Syntax Description

ip-address	(Optional) Specific IP address.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to clear all entries in the cache.

Examples

The following example displays output from this command:

```
Router# show call fallback cache

Probe   IP Address      Codec   Delay   Loss    ICPIF   Reject  Accept
-----   ----------      -----   -----   ----    -----   ------  ------
1       1.1.1.4         g729r8  40      00       0       9
2       122.24.56.25    g729r8  14810      5       1       4

2 active probes

Field                     Description
-------                   ------------
Probe                     Probe number
IP Address                IP Address to which the probe is sent
Codec                     Codec Type of the probe
Delay                     Delay in milliseconds that the probe incurred
Loss                      Loss in % that the probe incurred
ICPIF                     Computed ICPIF value for the probe
Reject                    Number of times that calls of Codec Type <Codec>
                          were rejected to the IP Address
Accept                    Number of times that calls of Codec Type <Codec>
                          were accepted to the IP Address
active probes             Number of destinations being probed
```

```
Router# show call fallback cache 10.14.115.53

Probe   IP Address      Codec           ICPIF   Reject  Accept
-----   ----------      -----           -----   ------  ------
1       10.14.115.53     g729r8          0       0       2

1 active probes
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show call fallback stats	Displays call fallback statistics.

show call fallback config

To display the call fallback configuration, use the **show call fallback config** command in EXEC mode.

show call fallback config

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example displays output from the **show call fallback config** command:

```
Router# show call fallback config

VoIP fallback config:
Fallback is ON
Using ICPIF threshold:
        ICPIF value timeout:20 seconds
        ICPIF threshold:20
Number of packets in a probe:20
IP precedence of probe packets:2
Fallback cache size:2 entries
Fallback cache timeout:240 seconds
Instantaneous value weight:65
MD5 Keychain:secret
```

Table 67 describes the fields shown in the **show call fallback config** display

Table 67 show call fallback config Field Descriptions

Field	Description
Fallback is	Lists enabled/disabled state of call fallback.
Using ICPIF threshold	ICPIF is configured to determine network traffic.
ICPIF value timeout	Lists probe timeout for collecting ICPIF information.
ICPIF threshold	Lists configured ICPIF threshold.
Number of packets in a probe	Lists number of configured packets per probe.
IP precedence of probe packets	Lists configured IP precedence for probes.
Fallback cache size	Number of allowed entries in call fallback cache.
Fallback cache timeout	Length of cache timeout, in seconds.

Table 67 show call fallback config Field Descriptions (continued)

Field	Description
Instantaneous value weight	Lists weight configured for calculating cache entry based on new probe and last entry.
MD5 Keychain	MD5 authentication has been configured with a keychain of *secret*.

Related Commands

Command	Description
call fallback monitor	Enables the monitoring of destinations without fallback to alternate dial peers.
show voice trunk-conditioning signaling	Enables fallback to alternate dial peers in case of network congestion.

show call fallback stats

To display the call fallback statistics, use the **show call fallback stats** command in EXEC mode.

show call fallback stats

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

To remove all values, use the **clear call fallback stats** command.

Examples

The following example displays output from the **show call fallback stats** command:

```
Router# show call fallback stats

VOIP Fallback Stats:
Total accepted calls:3
Total rejected calls:1
Total cache overflows:1

Field                     Description
-------                   ------------
Total accepted calls      Number of times that calls were successful over IP.
Total rejected calls      Number of times that calls were rejected over IP.
Total cache overflows     Number of times that the fallback cache overflowed and required
pruning.
```

Table 68 describes the fields shown in the **show call fallback stats** display

.

Table 68 show call fallback stats Fields with Descriptions

Field	Description
Total accepted calls	Number of times that calls were successful over IP.
Total rejected calls	Number of times that calls were rejected over IP.
Total cache overflows	Number of times that the fallback cache overflowed and required pruning.

Related Commands

Command	Description
clear call fallback stats	Clears the call fallback statistics.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.

show call filter components

To display the components used for filtering calls, use the **show call filter components** command in privileged EXEC mode.

show call filter components

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the output from running the **show call filter components** command. The GCFM is the generic call filter module, which is the internal module that controls which components are filtered:

```
Router# show call filter components
 The following components registered in GCFM:
     ISDN
     VTSP
     CCAPI
     TGRM
     DIAL-PEER
     NUMBER-TRANSLATION
     SSAPP
     VOICE-IVR-V2
     H323
     SIP
     CRM
```

Table 69 describes the significant fields shown in the display.

Table 69 show call filter components Field Descriptions

Field	Description
The following components registered in GCFM:	Shows which components are filtered in the generic call filter module.

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug call filter inout	Display the debug trace inside the GCFM.
debug condition match-list	Run a filtered debug on a voice call.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

show call filter match-list

To display call filter match lists, use the **show call filter match-list** command in privileged EXEC mode.

show call filter match-list *tag*

Syntax Description		
	tag	Numeric label that uniquely identifies the match list.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(4)T	This command was introduced.

Examples The following example shows an output from the **show call filter match-list** command:

```
Router# show call filter match-list

****************************************
call filter match-list 9 voice
****************************************
  incoming calling-number 50200
  incoming called-number 50201
  incoming signal local ipv4 10.0.101.22
  incoming signal remote ipv4  10.0.101.21
  incoming media local ipv4  10.0.101.22
  incoming media remote ipv4  10.0.101.21
  incoming dialpeer 502
  outgoing calling-number 50200
  outgoing called-number 50201
  outgoing port 6/0:D
  outgoing dialpeer 501
 debug condition match-list is set to EXACT_MATCH
****************************************
call filter match-list 10 voice
****************************************
  incoming calling-number 50300
  incoming called-number 50301
  incoming signal local ipv4 10.0.101.22
  incoming signal remote ipv4  10.0.101.21
  incoming media local ipv4  10.0.101.22
  incoming media remote ipv4  10.0.101.21
  incoming dialpeer 504
  outgoing calling-number 50300
  outgoing called-number 50301
  outgoing port 6/1:D
  outgoing dialpeer 503
 debug condition match-list is set to EXACT_MATCH
```

Table 70 describes the significant fields shown in the display.

Table 70 show call filter match-list Field Descriptions

Field	Description
call filter match-list 9 voice	Shows which match list is being displayed.
debug condition match-list is set to EXACT_MATCH	Shows whether the debug condition is set for exact match or partial match.

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug call filter inout	Display the debug trace inside the GCFM.
debug condition match-list	Run a filtered debug on a voice call.
show call filter components	Display the components used for filtering calls.

show call history fax

To display the call history table for fax transmissions, use the **show call history fax** command in user EXEC or privileged EXEC mode.

show call history fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *time*] | **id** *identifier* | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version.
duration *time*	(Optional) Displays history information for calls that are longer or shorter than a specified *time* value. The arguments and keywords are as follows: • **less**—Displays calls shorter than the value in the *time* argument. • **more**—Displays calls longer than the value in the *time* argument. • *time*—Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. Range is from 1 to 100.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was modified. The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was modified. The **brief** keyword was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	This command was modified. The output of this command was modified to indicate whether the call in question has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 was not included in this release.

Release	Modification
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(1)	This command was modified. The following fields were added: FaxRelayMaxJitterBufDepth, FaxRelayJitterBufOverFlow, FaxRelayHSmodulation, and FaxRelayNumberOfPages.
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

This command displays a call-history table that contains a list of fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is sample output from the **show call history fax** command:

```
Router# show call history fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1


GENERIC:
SetupTime=590180 ms
Index=2
PeerAddress=4085452930
PeerSubAddress=
PeerId=81
PeerIfIndex=221
LogicalIfIndex=145
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=59389
DisconnectTime=68204
```

```
CallDuration=00:01:28
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=295
TransmitBytes=5292
ReceivePackets=2967
ReceiveBytes=82110
TELE:
ConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
IncomingConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=28960 ms
VoiceTxDuration=0 ms
FaxTxDuration=28960 ms
FaxRate=voice bps
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
NoiseLevel=-120
ACOMLevel=127
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550130
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
```

Table 69 provides an alphabetical listing of the fields displayed in the output of the **show call history fax** command and a description of each field.

Table 69 show call history fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.

Table 69 show call history fax Field Descriptions (continued)

Field	Description
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallerName	Voice port station name string.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
DisconnectCause	Cause code for the reason this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time, in ms, when this call was disconnected.
EchoCancellerMaxReflector=64	The location of the largest reflector, in ms. The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
FaxRelayJitterBufOverFlow	Count of number of network jitter buffer overflows (number of packets). These packets are equivalent to lost packets.
FaxRelayMaxJitterBufDepth	Maximum depth of jitter buffer (in ms).
FaxRelayHSmodulation	Most recent high-speed modulation used.
FaxRelayNumberOfPages	Number of pages transmitted.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.

Table 69 show call history fax Field Descriptions (continued)

Field	Description
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
GwReceivedCalledNumber, GwReceivedCalledOctet3, GwReceivedCallingNumber, GwReceivedCallingOctet3, GwReceivedCallingOctet3a	Call information received at the gateway.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call.
ImgPages	The fax pages that have been processed.
Incoming ConnectionId	The incoming_GUID. It can be different with ConnectionId (GUID) when there is a long_pound or blast_call feature involved. In those cases, incoming_GUID is unique for all the subcalls that have been generated, and GUID is different for each subcall.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.

Table 69 show call history fax Field Descriptions (continued)

Field	Description
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, as well as octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.

Table 69 show call history fax Field Descriptions (continued)

Field	Description
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalled Number, TranslatedRedirectCalledOctet	Translated call information.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call history fax brief** command:

```
Router# show call history fax brief

<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
 tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

2    : 5996450hs.25 +-1 +3802 pid:100 Answer 408
 tx:0/0 rx:0/0 1F  (T30 T1 EOM timeout)
 Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm

2    : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
 tx:0/0 rx:0/0 3F  (The e-mail was not sent correctly. Remote SMTP server said: 354 )
 IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0

3    : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
 tx:11/14419 rx:0/0 10  (Normal connection)
 Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm

3    : 6447780hs.28 +1182 +4516 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

4    : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
```

```
 tx:11/14413 rx:0/0 10  (Normal connection)
 Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm

4    : 6464748hs.30 +1118 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

5    : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
 tx:0/0 rx:3/3224 10  (Normal connection)
 Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm

5    : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
 tx:0/2754 rx:0/0 3F  (service or option not available, unspecified)
 IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0

6    : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
 tx:11/14447 rx:0/0 10  (Normal connection)
 Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm

6    : 6517106hs.34 +1149 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

7    : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
 tx:11/14411 rx:0/0 10  (Normal connection)
 Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm

7    : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
```

The following example shows output for the **show call history fax** command with the T.38 Fax Relay statistics:

```
Router# show call history fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1


GENERIC:
SetupTime=9872460 ms
Index=8
PeerAddress=41023
PeerSubAddress=
PeerId=1
PeerIfIndex=242
LogicalIfIndex=180
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=9875610 ms
DisconnectTime=9936000 ms
CallDuration=00:01:00 sec
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=268
TransmitBytes=4477
ReceivePackets=1650
ReceiveBytes=66882
```

```
TELE:
ConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
IncomingConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
CallID=7
Port=3/0/0:0 (7)
BearerChannel=3/0/0.8
TxDuration=6170 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitterBufDepth=560 ms
FaxRelayJitterBufOverFlow=0
FaxRelayMostRecentHSmodulation=V.17/short/14400
FaxRelayNumberOfPages=1
FaxRelayInitHSmodulation=V.17/long/14400
FaxRelayDirection=Transmit
FaxRelayPktLossConceal=0
FaxRelayEcmStatus=ENABLED
FaxRelayEncapProtocol=T.38 (UDPTL)
FaxRelayNsfCountryCode=Japan
FaxRelayNsfManufCode=0031B8EE80C48511DD0D0000DDDD0000DDDD00000000000000000022ED00B0A400
FaxRelayFaxSuccess=Success
NoiseLevel=0
ACOMLevel=0
SessionTarget=
ImgPages=0
CallerName=Analog 41023
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x80
OriginalCalledNumber=41021
OriginalCalledOctet=0xA1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=41023
TranslatedCallingOctet=0x80
TranslatedCalledNumber=41021
TranslatedCalledOctet=0xA1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=41021
GwReceivedCalledOctet3=0xA1
```

Table 70 describes the fields not shown in Table 69.

Table 70 show call history fax Field Descriptions

Field	Description
FaxRelayDirection	Direction of fax relay.
FaxRelayEcmStatus	Fax relay error correction mode status.
FaxRelayEncapProtocol	Fax relay encapsulation protocol.
FaxRelayFaxSuccess	Fax relay success.
FaxRelayInitHSmodulation	Fax relay initial high speed modulation.
FaxRelayMostRecentHSmodulation	Fax relay most recent high speed modulation.
FaxRelayNsfCountryCode	Fax relay Nonstandard Facilities (NSF) country code.
FaxRelayNsfManufCode	Fax relay NSF manufacturers code.
FaxRelayPktLossConceal	Fax relay packet loss conceal.

Related Commands

Command	Description
dial-control-mib	Specifies attributes for the call history table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history voice	Displays the call history table for voice calls.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call history media

To display the call history table for media calls, use the **show call history media** command in user EXEC or privileged EXEC mode.

show call history media [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds* | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of the call history table.
duration	(Optional) Displays the call history for the specified time duration.
less	Displays the call history for shorter duration calls.
more	Displays the call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. The range is from 1 to 100.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command displays a call-history table that contains a list of media calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

When a media call is active, you can display its statistics by using the **show call active media** command.

Examples

The following is sample output from the **show call history media** command:

```
Router# show call history media

Telephony call-legs: 0
```

```
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Media call-legs: 4
Total call-legs: 4


GENERIC:
SetupTime=308530 ms
Index=4
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=309440 ms
DisconnectTime=320100 ms
CallDuration=00:00:10 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=237
TransmitBytes=37920
ReceivePackets=0
ReceiveBytes=0
VOIP:
ConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
IncomingConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
CallID=14
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=2FBDA670-C3511DB-8015C48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=3000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=2740 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=40 ms
```

```
Source tg label=test5
ReceiveDelay=90 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=

GENERIC:
SetupTime=308520 ms
Index=5
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=309370 ms
DisconnectTime=320100 ms
CallDuration=00:00:10 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=551
ReceiveBytes=88160
VOIP:
ConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
IncomingConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
CallID=13
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
```

```
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=2FBC6E20-C3511DB-8013C48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=7000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=2740 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=40 ms
Source tg label=test5
ReceiveDelay=95 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0102
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0103
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=

GENERIC:
```

```
SetupTime=408050 ms
Index=7
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=408160 ms
DisconnectTime=426260 ms
CallDuration=00:00:18 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=598
TransmitBytes=95680
ReceivePackets=0
ReceiveBytes=0
VOIP:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=19
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=6B0E94CD-C3511DB-801DC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=11000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=9560 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=55 ms
Source tg label=test5
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
```

```
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=

GENERIC:
SetupTime=408040 ms
Index=8
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=408130 ms
DisconnectTime=426260 ms
CallDuration=00:00:18 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=911
ReceiveBytes=145760
VOIP:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=18
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
```

```
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=sipv2
ProtocolCallId=6B0CC055-C3511DB-801BC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=9000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=9560 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=55 ms
Source tg label=test5
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=
```

Table 71 describes the significant fields shown in the display, in alphabetical order.

Table 71 show call history media Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: not answer or originate.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) Delay during this call, in ms.
Index	Dial peer identification number.
InfoType	Information type for this call; for example, voice, speech, or fax.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.

Table 71 show call history media Field Descriptions (continued)

Field	Description
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
VAD	Whether voice activation detection (VAD) was enabled for this call.

Related Commands

Command	Description
dial-control-mib	Sets the maximum number of calls contained in the table.
show call active media	Displays call information for media calls in progress.

show call history video

To display call history information for signaling connection control protocol (SCCP) video calls, use the **show call history video** command in user EXEC or privileged EXEC mode.

show call history video [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of video call history information.
id *identifier*	(Optional) Displays only the video call history with the specified identifier. Range is a hexadecimal value from 1 to FFFF.
compact	(Optional) Displays a compact version of video call history information.
duration	(Optional) Displays the call history for the specified time duration.
less	Displays the call history for shorter duration calls.
more	Displays the call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. The range is from 1 to 100.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(4)XC	Cisco Unified CME 4.0	This command was introduced.
12.4(9)T	Cisco Unified CME 4.0	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(16); 12.4(15)T	Cisco Unified CME 4.0	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.

Examples

The following is sample output from the **show call history video** command with the **compact** option:

```
Router# show call history video compact

      <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       241      ANS     T17    g729r8      VOIP        P555-0100          192.0.2.0:16926
       242      ORG     T17    g729r8      TELE-VIDEO  P555-0101
```

Table 72 describes the significant fields shown in the display.

Table 72 show call history video Field Descriptions

Field	Description
callID	Unique identifier for the call leg.
A/O	Call leg was an answer (ANS) or an originator (ORG).
FAX	Fax number for the call leg.
T<sec>	Duration in seconds.
Codec	Codec used for this call leg.
type	Call type for this call leg.
Peer Address	Called or calling number of the remote peer.
IP R<ip>:<udp>	IP address and port number
Total call-legs	Total number of call legs for this call.

Related Commands

Command	Description
show call active video	Displays call information for SCCP video calls in progress.

show call history video record

To display information about incoming and outgoing video calls, use the **show call history video record** command in privileged EXEC mode.

show call history video record

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example displays information about two video calls:

```
Router# show call history video record

CallId = 4
CalledNumber = 221
CallDuration = 39006 seconds
DisconnectText = remote hangup
SVC: call ID = 8598630
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 414, vpi = 0, vci = 158
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
CallId = 3
CalledNumber = 221
CallDuration = 557 seconds
DisconnectText = local hangup
SVC: call ID = 8598581
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 364, vpi = 0, vci = 108
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
```

show call history voice

To display the call history table for voice calls, use the **show call history voice** command in user EXEC or privileged EXEC mode.

show call history voice [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **id** *identifier* | **last** *number* | **redirect** {**rtpvt** | **tbct**} | **stats**]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is from 1 to FFFF.
compact	(Optional) Displays a compact version of the call history table.
duration *seconds*	(Optional) Displays history information for calls that are longer or shorter than the value of the specified *seconds* argument. The arguments and keywords are as follows: • **less**—Displays calls shorter than the *seconds* value. • **more**—Displays calls longer than the *seconds* value. • *seconds*—Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. Range is from 1 to 100.
redirect	(Optional) Displays information about calls that were redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT). The keywords are as follows: • **rtpvt**—Displays information about RTPvt calls. • **tbct**—Displays information about TBCT calls.
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	Support was added for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(5)XK	This command was implemented on the Cisco MC3810.
12.0(7)XK	The **brief** keyword was implemented on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Release	Modification
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	The output of this command was modified to indicate whether a specified call has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(11)T	Support was added for Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	The ReleaseSource field was added to the Field Description table, and the **record** keyword was deleted from the command name.
12.3(1)	The **redirect** keyword was added.
12.4(2)T	The LocalHostname display field was added to the VoIP call leg record.
12.4(11)XW	The **stats** keyword was added.
12.4(15)T	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	Command output was updated to show IPv6 information.

Usage Guidelines

This command displays a call-history table that contains a list of voice calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed. The timer value is also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

Use the **show call active voice redirect** command to review records for calls that implemented RTPvt or TBCT.

When a call is active, you can display its statistics by using the **show call active voice** command.

Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice

GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
```

```
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=2
RemoteIPAddress=10.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
SessionTarget=ipv4:10.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas

Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
```

```
DisconectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=3
Port=3/0/0 (3)
BearerChannel=3/0/0.1
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0
```

The following example from a Cisco AS5350 router displays a sample of voice call history records showing release source information:

```
Router# show call history voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Total call-legs: 2

GENERIC:
SetupTime=85975291 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.

.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
VOIP:
ConnectionId[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=1
.
.
```

```
.
GENERIC:
SetupTime=85975290 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975336
DisconnectTime=85979340
CallDuration=00:00:40
CallOrigin=2
ReleaseSource=1
.
.
.
TELE:
ConnectionId=[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief

<ID>: <CallID> <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm
acom:<lvl>dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
disc:<cause code>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

The following is sample output from the **show call history voice redirect** command:

```
Router# show call history voice redirect tbct

index=2, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=3, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=4, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12
index=5, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12

Number of call-legs redirected using tbct with notify:4
```

Table 73 describes the significant fields shown in the **show call history voice redirect tbct** display.

Table 73 show call history voice redirect Field Descriptions

Field	Description
index	Index number of the record in the history file.
xfr	Whether TBCT or TBCT with notify has been invoked.
status	Status of the redirect request.
start_time	Time, in hours, minutes, and seconds when the redirected call began.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
Number of call-legs redirected using tbct with notify	Total number of call legs that were redirected using TBCT with notify.

Related Commands

Command	Description
dial-control-mib	Set the maximum number of calls contained in the table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history fax	Displays the call history table for fax transmissions.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call language voice

To display a summary of languages configured and the URLs of the corresponding Tool Command Language (TCL) modules for the languages that are not built-in languages, use the **show call language voice command in** EXEC mode.

show call language voice [*language* | **summary**]

Syntax Description

language	(Optional) Two-character prefix configured with the **call language voice** command in global configuration mode, either for a prefix for a built-in language or one that you have defined; for example, “en” for English or “ru” for Russian.
summary	(Optional) Summary of all the languages configured and the URLs for the TCL modules other than built-in languages.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

This command is similar to the **show call application voice** command. If a language is built in, the URL listed reads “fixed.” If you decide to overwrite the built-in language with your own language, the word “fixed” in the URL column changes to the actual URL where your new application lives.

Examples

The following command displays a summary of the configured languages:

```
Router# show call language voice summary

name       url
sp         fixed
ch         fixed
en         fixed
ru         tftp://dirt/fwarlau/scripts/multilag/ru_translate.tcl
```

The following command displays information about Russian-language configuration:

```
Router# show call language voice ru

ru_translate.tcl
ru_translate.tcl~
singapore.cfg
test.tcl
people% more ru_translate.tcl
# Script Locked by: farmerj
# Script Version: 1.1.0.0
# Script Lock Date: Sept 24 2000
# ca_translate.tcl
#-----------------------------------------------------------------
# Sept 24, 2000 Farmer Joe
#
```

```
# Copyright (c) 2000 by Cisco Systems, Inc.
# All rights reserved.
#------------------------------------------------------------------
#<snip>...
...set prefix ""
#puts "argc"

#foreach arg $argv {
#puts "$arg"

#    translates $arg

#    puts "\t\t**** $prompt RETURNED"
#}
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
call language voice	Configures a TCL module.
call language voice load	Loads or reloads a TCL module from the configured URL location.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
show call application voice	Shows and describes applications.

show call leg

To display event logs and statistics for voice call legs, use the **show call leg** command in privileged EXEC mode.

show call leg {**active** | **history**} [**summary** | [**last** *number* | **leg-id** *leg-id*] [**event-log** | **info**]]

Syntax Description

active	Statistics or event logs for active call legs.
history	Statistics or event logs for terminated call legs.
summary	(Optional) A summary of each call leg.
last *number*	(Optional) Selected number of most recent call legs. Not available with **active** keyword.
leg-id *leg-id*	(Optional) A specific call leg. Output displays event logs or statistics for that call leg.
event-log	(Optional) Event logs for call legs.
info	(Optional) Statistics for call legs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you use the **leg-id** keyword, only statistics or event logs for that call leg display. To display event logs with this command, you must enable event logging with the **call leg event-log** command.

Examples

The following is sample output from the **show call leg** command using different keywords:

```
Router# show call leg active summary

G<id>  L<id>     Elog A/O FAX T<sec> Codec       type  Peer Address       IP R<ip>:<udp>
G11DC  L A        Y   ANS     T2     None        TELE  P4085550198

Total call-legs: 1

Router# show call leg active event-log

Event log for call leg ID: A        Connection ID: 11DC
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None

Total call-legs: 1
```

```
Router# show call leg active info

Information for call leg ID: A        Connection ID: 11DC

 GENERIC:
SetupTime=3012940 ms
Index=1
PeerAddress=4085550198
PeerSubAddress=
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
ConnectTime=301295
CallDuration=00:00:20
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=412
TransmitBytes=98880
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
OutSignalLevel=-50
InSignalLevel=-41
InfoActivity=0
ERLLevel=38
EchoCancellerMaxReflector=16685
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81
Total call-legs: 1
```

For a description of the call leg statistics, see the description for the **show call active voice** command.

```
Router# show call leg active leg-id A

Call Information - Connection ID: 11DC , Call Leg ID: A
```

```
 GENERIC:
SetupTime=3012940 ms
Index=1
PeerAddress=4085550198
PeerSubAddress=
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
ConnectTime=301295
CallDuration=00:00:40
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=824
TransmitBytes=197760
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
OutSignalLevel=-50
InSignalLevel=-41
InfoActivity=0
ERLLevel=38
EchoCancellerMaxReflector=16685
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
```

```
Call-leg found: 1

Router# show call leg active leg-id A event-log

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None

Call-leg found: 1

Router# show call leg history summary

G<id>  L<id>     Elog A/O FAX T<sec> Codec       type  Peer Address       IP R<ip>:<udp>
disc-cause
G11DB  L 7        Y   ANS     T24    None        TELE  P4085550198 D10
G11DC  L A        Y   ANS     T159   None        TELE  P4085550198 D10

Total call-legs: 2

Router# show call leg history last 1

Call Information - Connection ID: 11DC , Call Leg ID: A


GENERIC:
SetupTime=3012940 ms
Index=4
PeerAddress=4085550198
PeerSubAddress=
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=301295
DisconnectTime=317235
CallDuration=00:02:39
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2940
TransmitBytes=705600
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
```

```
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
A:1057277860:150:INFO: Inform application call disconnected (cause = normal call clearing
(16))
A:1057277860:154:INFO: Call disconnected (cause = normal call clearing (16))
A:1057277860:155:INFO: Call released

Total call-legs: 1
Total call-legs with event log: 1

Router# show call leg history leg-id A event-log

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
A:1057277860:150:INFO: Inform application call disconnected (cause = normal call clearing
(16))
A:1057277860:154:INFO: Call disconnected (cause = normal call clearing (16))
A:1057277860:155:INFO: Call released

Call-leg matched ID found: 1
Call-legs matched ID with event log: 1
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.

Command	Description
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.

show callmon

To display call monitor information, use the **show callmon** command in user EXEC or privileged EXEC mode.

show callmon {**call** | **gcid** | **subscription** | **trace** {**all** | **event** {**all** | **call** | **connection**} | **exec** | **server** | **subscription** | **trigger**}}

Syntax Description

call	Displays the active call monitor calls.
gcid	Displays the active global call ID information.
subscription	Displays the subscription information.
trace	Displays the trace information.
all	Displays all types of traces based on time.
event	Displays the event trace information. • **all**—Displays all event traces. • **call**—Displays event traces related to a call. • **connection**—Displays the event traces related to a connection.
exec	Displays all critical execution traces.
server	Displays all session server up or down traces.
subscription	Displays all subscription traces.
trigger	Displays the entire trigger structure by index.

Command Modes

User EXEC (>)
Privileged EXEC (#))

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following sample output from the **show callmon call** command shows active call monitor calls:

```
Router# show callmon call

 line dn     sub_id   number of call instance
6401,     1
      callID 2038(19D7),  *cg = 6401, cd = 6601
6601,     1
      callID 2039(19D7),  cg = 6401, *cd = 6601
```

Table 74 describes the significant fields shown in the display.

Table 74 show callmon call Field Descriptions

Field	Description
dn	Directory number.
number of call	Number of call instances.
instance	Contents of the call instance.

The following sample output from the **show callmon gcid** command shows the active global call ID information:

```
Router# show callmon gcid

 GCID                                callIDs(active_entry_id)
AE48ECBC-D89311DB-87FC996E-115FF692
 isConfGcid:FALSE        gcid_conf:00000000-00000000-00000000-00000000
, 2038(19D7), 2039(19D7)
```

Table 75 describes the significant fields shown in the display.

Table 75 show callmon gcid Field Descriptions

Field	Description
GCID	Global call ID.
CallIDs	Active call IDs.

Related Commands

Command	Description
callmonitor	Enables call monitoring messaging functionality on a SIP endpoint in a VoIP network.

show call prompt-mem-usage

To display the amount of memory used by prompts, use the **show call prompt-mem-usage** command in privileged EXEC mode.

show call prompt-mem-usage [**detail**]

Syntax Description		
	detail	(Optional) Displays details about memory usage and names of tones used.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.3(7)T	The **detail** keyword was added.

Usage Guidelines Use this command to display the number of prompts loaded into the gateway, the amount of memory used by the prompts, the number of prompts currently being played, and the status of prompt loads.

For calls transferred by a Cisco CallManager Express (Cisco CME) system, the ringback tone generation for commit-at-alerting uses an interactive voice response (IVR) prompt playback mechanism. Ringback tone is played to the transferred party by the Cisco CME system associated with the transferring party.

The system automatically generates tone prompts as needed on the basis of the network-locale setting made in the Cisco CME system.

Examples The following sample output shows details about the memory usage of the prompts that are used.

```
Router# show call prompt-mem-usage

Prompt memory usage:
             config'd      wait    active      free     mc total    ms total
    file(s)      0200      0010      0001     00189        00011       00002
    memory   02097152  00081259  00055536  01960357     00136795

 Prompt load counts: (counters reset 0)
    success 11(1st try) 0(2nd try), failure 0

 Other mem block usage:
            mcDynamic   mcReader
    gauge       00001      00001

Number of prompts playing: 1
Number of start delays   : 0
MCs in the ivr MC sharing table
==============================
Media Content: NoPrompt (0x83C64554)
  URL:
  cid=0, status=MC_READY size=24184 coding=g711ulaw refCount=0
Media Content: tone://GB_g729_tone_ringback (0x83266EC8)
  URL: tone://GB_g729_tone_ringback
```

Table 76 describes the significant fields shown in the display.

Table 76 show call prompt-mem-usage Field Descriptions

Field	Description
file(s)	Number of prompts in different queues.
file(s) - config'd	Maximum number of configured prompts that can be simultaneously available in memory. In the sample output, the value of 200 in this field means that loading the 201st prompt results in the oldest prompts being removed.
file(s) -wait	Number of prompts in the wait queue that are not being used in any call and are ready to be deleted when there is no space for a new prompt. This field lists older prompts that can be deleted.
file(s) - active	Number of prompts that are being used in active calls. These prompts cannot be deleted.
file(s) - free	Number of prompts that can be loaded without deleting any prompt from the wait queue. This is the number of configured prompts (listed under config'd) minus the total number of prompts in the wait and active states.
file(s) - mc total	Total number of prompts in the wait and active states.
ms total	Number of media streams that are currently active. One media stream is used for playing INBOX prompts. A prompt is considered an INBOX prompt if its URL is either flash:, http:, ram:, or tftp:.
memory	Displays the memory used by prompts, in bytes.
memory - config'd	Maximum amount of memory configured to be available for prompts.
memory - wait	Total amount of memory used by prompts in the wait list.
memory - active	Total amount of memory used by prompts in the active list.
memory - free	Amount of available memory. This is the amount of configured prompts (listed under config'd) memory minus the total amount of memory used by the prompts in the wait and active lists.
memory - mc total	Total amount of memory used by prompts in the wait and active lists.
Prompt load counts	Number of successful attempts to load a prompt on the first try and on the second try, and the number of attempts to load a prompt that failed.
mcDynamic	Number of dynamic element queues that are active. A dynamic element queue is a list of prompts that are played together.
mcReader	Number of mcReaders that are active. An mcReader is used for playing one mcDynamic queue of prompts. An mcReader is used only if the mcDynamic contains prompts that are associated with one of the following types of URL: flash:, http:, ram:, or tftp:.
Number of prompts playing	Number of prompts that are currently playing.
Number of start delays	Number of times that prompts failed to start and have subsequently restarted.
MCs in the ivr MC sharing table	The fields below this line of text refer to each media content (prompt) currently cached in memory. In the sample output, the only cached prompt is the built-in default prompt named "NoPrompt."

Table 76 show call prompt-mem-usage Field Descriptions (continued)

Field	Description
Media Content	Name of the prompt, which is derived from the audio file URL (the characters after the last "/" in the URL). The address in parentheses is the memory location of the prompt.
URL	Location of the file for the prompt that is playing. In the case of the default prompt, NoPrompt, no URL is given.
cid	Call identification number of the call that initiated the loading of the prompt.
status	Status of the media content. The following values are possible: • MC_NOT_READY—Initial status for media content. When the media content is successfully loaded, the status will change to MC_READY. • MC_READY—Media content is loaded into memory and ready for use. • MC_LOAD_FAIL—Media content failed to load.
size	Size of the media content, in bytes.
coding	Type of encoding used by the media content.
refCount=0	Number of calls to which this media content is currently being streamed.

show call resource voice stats

To display resource statistics for an H.323 gateway, use the **show call resource voice stats** command in privileged EXEC mode.

show call resource voice stats [**ds0** | **dsp**]

Syntax Description

ds0	(Optional) Specifies the voice digital signal level zero (DS0) resource statistics information.
dsp	(Optional) Specifies the voice digital signal processor (DSP) resource statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was integrated into Cisco IOS Release into 12.2(2)XB1.
12.2(8)T	This command was modified. Support for the Cisco AS5300,Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 series routers is not included in this release.
12.4(22)T	This command was modified. The **ds0** and **dsp** keywords were added.

Usage Guidelines

The **show call resource voice stats** command displays the H.323 resources that are monitored when the **resource threshold** command is used to configure resource threshold reporting.

Note Cisco 4000 Series Integrated Services Routers do not support this command.

Examples

The following is sample output from the show call resource voice stats command, which shows the resource statistics for an H.323 gateway:

```
Router# show call resource voice stats

Resource Monitor -  Dial-up Resource Statistics Information:

DSP Statistics:

Utilization: 0 percent
Total channels: 48
Inuse channels: 0
Disabled channels 0:
Pending channels: 0
Free channels: 48
```

```
DS0 Statistics:
```

```
Total channels: 0
Addressable channels: 0
Inuse channels: 0
Disabled channels: 0
Free channels: 0
```

Table 77 describes significant fields shown in this output.

Table 77 show call resource voice stats Field Descriptions

Statistic	Definition
Total channels	Number of channels physically configured for the resource.
Inuse channels	Number of addressable channels that are in use. This value includes all channels that either have active calls or have been reserved for testing.
Disabled channels	Number of addressable channels that are physically down or that have been disabled administratively with the **shutdown** or **busyout** command.
Pending channels	Number of addressable channels that are pending in loadware download.
Free channels	Number of addressable channels that are free.
Addressable channels	Number of channels that can be used for a specific type of dialup service, such as H.323, which includes all the DS0 resources that have been associated with a voice plain old telephone service (POTS) dial plan profile.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.

show call resource voice threshold

To display the threshold configuration settings and status for an H.323 gateway, use the **show call resource voice threshold** command in privileged EXEC mode.

show call resource voice threshold [**ds0** | **dsp**]

Syntax Description

ds0	(Optional) Specifies the voice digital signal level zero (DS0) resource statistics information.
dsp	(Optional) Specifies the voice digital signal processor (DSP) resource statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2
12.2(2)XB1	This command was integrated into Cisco IOS Release into 12.2(2)XB1.
12.4(22)T	This command was modified. The **ds0** and **dsp** keywords were added.

Usage Guidelines

The **show call resource voice threshold** command displays the H.323 resource thresholds that are configured with the **resource threshold** command.

Note Cisco 4000 Series Integrated Services Routers do not support this command.

Examples

The following is sample output from the show call resource voice threshold command, which shows the resource threshold settings and status for an H.323 gateway:

```
Router# show call resource voice threshold

Resource Monitor -  Dial-up Resource Threshold Information:

DS0 Threshold:

Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: init
DSP Threshold:

Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: low_threshold_hit
```

Table 78 describes the significant fields shown in the display.

Table 78 show call resource voice threshold Field Descriptions

Field	Description
High Water Mark	Resource-utilization level that triggers a message indicating that H.323 resource use is high. The range is 1 to 100. A value of 100 indicates that the resource is unavailable.The default is 90.
Low Water Mark	Resource-utilization level that triggers a message indicating that H.323 resource use has dropped below the high-usage level. The range is 1 to 100. The default is 90.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice stats	Displays resource statistics for an H.323 gateway.

show call rsvp-sync conf

To display the configuration settings for Resource Reservation Protocol (RSVP) synchronization, use the **show call rsvp-sync conf** command in privileged EXEC mode.

show call rsvp-sync conf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XI1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco MC3810, Cisco AS5300, and Cisco AS5800.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300,Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following example shows sample output from this command:

```
Router# show call rsvp-sync conf

VoIP QoS: RSVP/Voice Signaling Synchronization config:

Overture Synchronization is ON
Reservation Timer is set to 10 seconds
```

Table 79 describes significant fields shown in this output.

Table 79 show call rsvp-sync conf Field Descriptions

Field	Description
Overture Synchronization is ON	Indicates whether RSVP synchronization is enabled.
Reservation Timer is set to xx seconds	Number of seconds for which the RSVP reservation timer is configured.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.

show call rsvp-sync stats

To display statistics for calls that attempted Resource Reservation Protocol (RSVP) reservation, use the **show call rsvp-sync stats** command in privileged EXEC mode.

show call rsvp-sync stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XI1	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows sample output from this command:

```
Router# show call rsvp-sync stats

VoIP QoS:Statistics Information:
Number of calls for which QoS was initiated   : 18478
Number of calls for which QoS was torn down   : 18478
Number of calls for which Reservation Success was notified : 0
Total Number of PATH Errors encountered : 0
Total Number of RESV Errors encountered : 0
Total Number of Reservation Timeouts encountered : 0
```

Table 80 describes significant fields shown in this output.

Table 80 show call rsvp-sync stats Field Descriptions

Field	Description
Number of calls for which QoS was initiated	Number of calls for which RSVP setup was attempted.
Number of calls for which QoS was torn down	Number of calls for which an established RSVP reservation was released.
Number of calls for which Reservation Success was notified	Number of calls for which an RSVP reservation was successfully established.
Total Number of PATH Errors encountered	Number of path errors that occurred.

Table 80 show call rsvp-sync stats Field Descriptions (continued)

Field	Description
Total Number of RESV Errors encountered	Number of reservation errors that occurred.
Total Number of Reservation Timeouts encountered	Number of calls in which the reservation setup was not complete before the reservation timer expired.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.

show call spike status

To display the configured call spike threshold and statistics for incoming calls, use the **show call spike status** command in privileged EXEC mode.

show call spike status [**dial-peer** *tag*]

Syntax Description

dial-peer	(Optional) Displays configuration information for a dial peer.
tag	(Optional) Specifies the dial peer identifying number. Range is from 1 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was added in this release.
15.1(3)T	This command was modified. The output fields of the command were modified to include the output at the dial peer level.

Examples

The following is sample output from this command:

```
Router# show call spike status

 Call Spiking:Configured
 Call spiking :NOT TRIGGERED
 total call count in sliding window ::20
```

Table 81 describes the significant fields shown in the display.

Table 81 show call spike status Field Descriptions

Field	Description
Call Spiking	Current enabled state of call spiking.

Table 81 show call spike status Field Descriptions (continued)

Call Spiking	Details if the call spiking limit has been triggered.
total call count in sliding window	Number of calls during the spiking interval.

```
Router# show call spike status dial-peer 400

TAG         CONFIG    SPIKED TOTAL REJECTED CALLS    REJECTED CALLS
400         YES       NO        4                        0
```

Table 82 describes the significant fields shown in the display.

Table 82 show call spike status (dial peer) Field Descriptions

Field	Description
TAG	Dial peer tag.
CONFIG	Displays if the **call spike** command has been configured.
SPIKED	Details if the call spiking limit has been triggered.
TOTAL REJECTED CALLS	Displays the number of calls rejected due to a call spike in the dial peer.
REJECTED CALLS	Displays the number of calls rejected when the call spike was triggered until the call spike control was released.

Related Commands

Command	Description
call spike	Configures the limit for the number of incoming calls in a short period of time.

show call threshold

To display enabled triggers, current values for configured triggers, and number of application programming interface (API) calls that were made to global and interface resources, use the **show call threshold** command in privileged EXEC mode.

show call threshold {**config** | **status** [**unavailable**] | **stats**}

Syntax Description

config	Displays the current threshold configuration.
status	Displays the status of all configured triggers and whether or not the CPU is available.
unavailable	(Optional) Displays the status for all unavailable resources.
stats	Displays statistics for API calls; that is, the resource-based measurement.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following is sample output from the **show call threshold config** command:

```
Router# show call threshold config

Some resource polling interval:
  CPU_AVG interval: 60
  Memory interval:  5

IF              Type            Value   Low     High    Enable
-----           ----            -----   ----    ----    ------
Serial3/1:23    int-calls       0       107     107     N/A
N/A             cpu-avg         0        70      90     busy&treat
```

The following is sample output from the **show call threshold status** command:

```
Router# show call threshold status

Status  IF              Type            Value   Low     High    Enable
------  ---             ------          ----    ----    ----    -----
Avail   N/A             total-calls     0       5       5000    busyout
Avail   N/A             cpu-avg         0       5       65      busyout
```

The following is sample output from the **show call threshold status unavailable** command:

```
Router# show call threshold status unavailable

Unavailable configured resources at the current time:
IF              Type            Value   Low     High    Enable
----            -----           -----   ----    ----    -----
```

The following is sample output from the **show call threshold stats** command:

```
Router# show call threshold stats

Total resource check: 0
 successful: 0
 failed:   0
```

Table 83 describes significant fields shown in this output.

Table 83 show call threshold Field Descriptions

Field	Description
CPU_AVG interval	Interval of configured trigger CPU_AVG.
Memory interval	Interval of configured trigger Memory.
IF	Interface.
Type	Type of resource.
Value	Value of call to be matched against low and high thresholds.
Low	Low threshold.
High	High threshold.
Enable	Shows if busyout and the **call treatment** command are enabled.

Related Commands

Command	Description
call threshold	Enables a resource and defines associated parameters.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.

show call treatment

To display the call-treatment configuration and statistics for handling the calls on the basis of resource availability, use the **show call treatment** command in privileged EXEC mode.

show call treatment {**config** | **stats**}

Syntax Description

config	Displays the call treatment configuration.
stats	Displays statistics for handling the calls on the basis of resource availability.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following is sample output from this command:

```
Router# show call treatment config

Call Treatment Config
---------------------

Call treatment is OFF.
Call treatment action is: Reject
Call treatment disconnect cause is: no-resource
Call treatment ISDN reject cause-code is: 41
```

Table 84 describes significant fields shown in this output.

Table 84 show call treatment config Field Descriptions

Field	Description
Call treatment is:	State of call treatment, either ON or OFF.
Call treatment action is:	Action trigger assigned for call treatment.

Table 84 show call treatment config Field Descriptions (continued)

Call treatment disconnect cause is:	Reason for disconnect.
Call treatment ISDN reject cause-code is:	Reject code number assigned.

The following is sample output from the **show call treatment** command:

```
Router# show call treatment stats

Call Treatment Statistics
-------------------------

Total Calls by call treatment: 0
Calls accepted by call treatment: 0
Calls rejected by call treatment: 0
Reason          Num. of calls rejected
------          ----------------------
cpu-5sec:       0
cpu-avg:        0
total-mem:      0
io-mem:         0
proc-mem:       0
total-calls:    0
```

Table 85 describes significant fields shown in this output.

Table 85 show call treatment stats Field Descriptions

Field	Description
Total Calls by call treatment:	Number of calls received and treated.
Calls accepted by call treatment:	Calls that passed treatment parameters.
Calls rejected by call treatment:	Calls that failed treatment parameters.
cpu-5sec	Number of calls rejected for failing the cpu-5sec parameter.
cpu-avg	Number of calls rejected for failing the cpu-avg parameter.
total-mem	Number of calls rejected for failing the total-mem parameter.
io-mem	Number of calls rejected for failing the io-mem parameter.
proc-mem	Number of calls rejected for failing the proc-mem parameter.
total-calls	Number of calls rejected for failing the total-calls parameter.

Related Commands

Command	Description
call treatment on	Enables call treatment to process calls when local resources are unavailable.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause-code for ISDN calls when local resources are unavailable.
clear call treatment stats	Clears the call-treatment statistics.

show call-router routes

To display the routes cached in the current border element (BE), use the **show call-router routes** in EXEC mode.

show call-router routes [**static** | **dynamic** | **all**]

Syntax Description

static	Descriptors provisioned on the border element.
dynamic	Dynamically learned descriptors.
all	Both static and dynamic descriptors.

Command Default All

Command Modes EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example is sample output from this command.

```
Router# show call-router routes

Static Routes:
==============
  DescriptorID= 6561676C650000000000000000000000A
  lastChanged = 19930301063311
   IP addr         :port       Prefix
   172.18.195.64   :2099       5553122

Dynamic Routes:
===============
  DescriptorID= 506174726F6E6F757300000000000000002
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       310

  DescriptorID= 506174726F6E6F757300000000000000003
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       555301

  DescriptorID= 506174726F6E6F757300000000000000004
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       555302
```

```
DescriptorID= 506174726F6E6F757300000000000005
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       818

  DescriptorID= 506174726F6E6F757300000000000001
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       1005
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show call-router active	Displays active call information for a voice call in progress.
show call-router history	Displays the VoIP call-history table.
show call-router status	Displays the Annex G BE status.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call-router status

To display the Annex G border element status, use the **show call-router status** command in user EXEC mode.

show call-router status [**neighbors**]

Syntax Description

neighbors	(Optional) Displays the neighbor border element status.

Command Modes

User EXEC

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and modified to add the **neighbors** keyword.

Examples

The following example displays the Annex G border element status. Note that the example shows the status for two neighbors.:

```
Router# show call-router status neighbors

ANNEX-G CALL ROUTER STATUS:
  ===========================
    Border Element ID Tag   : Celine
    Domain Name             : Celine-Domain
    Border Element State    : UP
    Border Element Local IP : 172.18.193.31:2099
    Advertise Policy        : STATIC descriptors
    Hopcount Value          : 7
    Descriptor TTL          : 3180
    Access Policy           : Neighbors only
    Current Active Calls    : 0
    Current Calls in Cache  : 0
    Cumulative Active Calls : 0
    Usage Ind Messages Sent : 0
    Usage Ind Cfm Rcvd      : 0
    IRRs Received           : 0
    DRQs Received           : 0
    Usage Ind Send Retrys   : 0

  NEIGHBOR INFORMATION:
  =====================
    Local Neighbor ID : (none)
    Remote Element ID : (unknown)
    Remote Domain ID  : (unknown)
    IP Addr           : 1.2.3.4:2099
    Status            : DOWN
    Caching           : OFF
    Query Interval    : 30 MIN (querying disabled)
```

```
Usage Indications :
  Current Active Calls : 0
  Retry Period         : 600 SEC
  Retry Window         : 3600 MIN
Service Relationship Status: ACTIVE
  Inbound Service Relationship  : DOWN
    Service ID     : (none)
    TTL            : 1200 SEC
  Outbound Service Relationship : DOWN
    Service ID     : (none)
    TTL            : (none)
    Retry interval : 120 SEC (0 until next attempt)
```

Table 86 describes significant fields shown in this output.

Table 86 show call-router status Field Descriptions

Field	Description
Border Element ID Tag	Identifier for the border element.
Border Element State	Indicates if the border element is running.
Border Element Local IP	Local IP address of the border element.
Advertise Policy	Type of descriptors that the border element advertises to its neighbors. Default is **static**. Other values are **dynamic** and **all**.
Hopcount Value	Maximum number of border element hops through which an address resolution request can be forwarded. Default is 7.
Descriptor TTL	Time-to-live value, or the amount of time, in seconds, for which a route from a neighbor is considered valid. Range is from 1 to 2147483647. Default is 1800 (30 minutes).
Access Policy	Requires that a neighbor be explicitly configured for requests to be accepted.
Local Neighbor ID	Domain name reported in service relationships.
Service Relationship Status	Service relationship between two border elements is active.
Inbound Service Relationship	Inbound time-to-Live (TTL) value in number of seconds. Range is from 1 to 4294967295.
Outbound Service Relationship	Specifies the amount of time, in seconds, to establish the outbound relationship. Range is from 1 to 65535.
Retry interval	Retry value between delivery attempts, in number of seconds. Range is from 1 to 3600.

Related Commands

Command	Description
advertise	Controls the type of descriptors that the border element advertises to its neighbors.
call-router	Enables the Annex G border element configuration commands.
hopcount	Specifies the maximum number of border element hops through which an address resolution request can be forwarded.
local	Defines the local domain, including the IP address and port border elements that the border element should use for interacting with remote border elements.

Command	Description
shutdown	Shuts down the Annex G border element.
ttl	Sets the expiration timer for advertisements.

show ccm-manager

To display a list of Cisco CallManager servers and their current status and availability, use the **show ccm-manager** command in privileged EXEC mode.

show ccm-manager [**backhaul** | **config-download** | **fallback-mgcp** | **hosts** | **music-on-hold** | **redundancy** | **download-tones** [**c1** | **c2**]]

Syntax Description

backhaul	(Optional) Displays information about the backhaul link.
config-download	(Optional) Displays information about the status of Media Gateway Control Protocol (MGCP) and Skinny Client Control Protocol (SCCP) configuration download.
fallback-mgcp	(Optional) Displays the status of the MGCP gateway fallback feature.
hosts	(Optional) Displays a list of each configured Cisco CallManager server in the network, together with its operational status and host IP address.
music-on-hold	(Optional) Displays information about all the multicast music-on-hold (MOH) sessions in the gateway at any given point in time.
redundancy	(Optional) Displays failover mode and status information for hosts, including the redundant link port, failover interval, keepalive interval, MGCP traffic time, switchover time, and switchback mode.
download-tones [**c1** | **c2**]	(Optional) Displays custom tones downloaded to the gateway. The custom tone value of c1 or c2 specifies which tone information to display.

Defaults

If none of the optional keywords is specified, information related to all keywords is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco CallManager Version 3.0 and Cisco VG200.
12.2(2)XA	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.2(2)XN	This command was modified to provide enhanced MGCP voice gateway interoperability to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11) and the Cisco CallManager Version 3.2. It was implemented on the Cisco IAD2420 series.
12.2(15)ZJ	The **download-tones** [**c1** | **c2**] keywords were added for the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(4)T	The keywords were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.3(14)T	New output was added relating to SCCP autoconfiguration.
12.4(15)XY	The display output was modified to include the number of TFTP download failures allowed.

Usage Guidelines

Use the **show ccm-manager config-download** command to determine the status of Cisco Unified Communications Manager servers and the automatic download information and statistics.

Examples

The following sample output shows the configured amplitudes, frequencies, and cadences of custom tone 1, Hong Kong:

```
Router# show ccm-manager download-tones c1
!
Custom Tone 1 : Hong Kong
Pulse dial:normal, Percent make:35%, DTMF low Amp.= 65424, high Amp.= 65446, Pcm:u-Law
                                        FXS  FXO  E&M  FXS  FXO  E&M
Dual Tone DR NF FOF FOS AOF AOF AOF AOS AOS AOS ONTF OFTF ONTS OFTS ONTT OFTT ONT4 OFT4
(optional) FOF2 FOS2 FOF3 FOS3 FOF4 FOS4 FOT FO4 AOT AO4 RCT1 RCT2 RCT3 RCT4
BUSY 0  2 480 620 -120 -120 -120 -120 -120 -120 500 500 0 0 0 0 0 0
RING_BACK           0  2   440   520 -120 -120 -120 -120 -120 -120   400   200   400  3000
CONGESTION          0  2   480   620 -200 -200 -200 -240 -240 -240   250   250     0     0
NUMBER_UNOBTAINABLE 0  2   480   620 -120 -120 -120 -120 -120 -120 65535     0     0     0
DIAL_TONE           0  2   350   440 -150 -150 -150 -150 -150 -150 65535     0     0     0
DIAL_TONE2          0  2   350   440 -150 -150 -150 -150 -150 -150 65535     0     0     0
OUT_OF_SERVICE      0  1   950     0 -150 -150 -150    0    0    0   330   330     0     0
ADDR_ACK            0  1   600     0 -240 -240 -240    0    0    0   125   125   125 65535
DISCONNECT          0  1   600     0 -150 -150 -150    0    0    0   330   330   330 65535
OFF_HOOK_NOTICE     0  2  1400  2040 -240 -240 -240 -240 -240 -240   100   100     0     0
OFF_HOOK_ALERT      0  2  1400  2040 -240 -240 -240 -240 -240 -240   100   100     0     0
WAITING             0  0     0     0    0    0    0    0    0    0     0     0     0     0
CONFIRM             0  0     0     0    0    0    0    0    0    0     0     0     0     0
CNFWRN_J            0  1   950     0 -170 -170 -190    0    0    0   100   100   100 65535
CNFWRN_D            0  1   600     0 -170 -170 -190    0    0    0   100   100   100 65535
STUTT_DIALTONE      0  2   350   440 -150 -150 -150 -150 -150 -150   100   100   100   100
100   100 65535     0
PERM_SIG_TONE       0  1   480     0 -170 -170 -170    0    0    0 65535     0     0     0
WAITING1            0  0     0     0    0    0    0    0    0    0     0     0     0     0
WAITING2            0  0     0     0    0    0    0    0    0    0     0     0     0     0
WAITING3            0  0     0     0    0    0    0    0    0    0     0     0     0     0
WAITING4            0  0     0     0    0    0    0    0    0    0     0     0     0     0
MSGWAIT_IND         0  0     0     0    0    0    0    0    0    0     0     0     0     0
OFF_HOOK_WARN       0  0     0     0    0    0    0    0    0    0     0     0     0     0
Sequence Tone       DR NF F1C1  F2C1   AOF   AOS  C1ONT C1OFT C2ONT C2OFT C3ONT C3OFT
C4ONT C4OFT  F1C2  F2C2  F1C3  F2C3  F1C4  F2C4
INTERCEPT           0  0     0     0     0     0      0     0     0     0     0     0
TONE_ON_HOLD        0  0     0     0     0     0      0     0     0     0     0     0
NO_CIRCUIT          0  0     0     0     0     0      0     0     0     0     0     0

Legend:
DR: direction NF: number of frequency FO<F,S,T,4>: frequency of<1st,2nd,3rd,4th>
AO<F,S,T,4>: amplitude of<1st,2nd,3rd,4th>
FOF<1-4>: frequency of 1st, cadence<1-4> FOS<1-4>: frequency of 2nd, cadence<1-4>
RCT<1-4>: repeat count for cadence<l-4>  F(1-4>C<1-4> : frequency<1-4> of cadence<1-4>
C<1-4>ONT: cadence<1-4> on time C<1-4>OFT: cadence<1-4> off time
```

Table 87, Table 88, and Table 89 give descriptions of significant fields once the tones are automatically downloaded to the gateway.

Table 87 show ccm-manager download-tones Significant Output Fields

Field	Description
Percent make	Pulse ratio in percentage of make.
DTMF low Amp.	Low frequency level.
high Amp.	High frequency level.
Pcm	Pulse Code Modulation (mu-law or a-law).

Table 88 show ccm-manager download-tones Output Fields for Dual Tones

Field of Dual Tone	Description
DR	Direction to PSTN (0) or Packet Network (1).
NF	Number of Frequency (from 1 to 4).
FOF	Frequency of First component (in Hz).
FXS AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the foreign exchange station (FXS).
FXO AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the foreign exchange office (FXO).
E&M AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the recEive and transMit (E&M).
FXS AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the FXS.
FXO AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the FXO.
E&M AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the E&M.
ONTF	On time; time the tone is generated (milliseconds) for the first frequency.
OFTF	Off time; silence time (milliseconds) for the first frequency.
ONTS	On time; time the tone is generated (milliseconds) for the second frequency.
OFTS	Off time; silence time (milliseconds) for the second frequency.
ONTT	On time; time the tone is generated (milliseconds) for the third frequency.
OFTT	Off time; silence time (milliseconds) for the third frequency.
ONT4	On time; time the tone is generated (milliseconds) for the fourth frequency.
OFT4	Off time; silence time (milliseconds) for the fourth frequency.
FOF2	Frequency of First component for the second cadence.
FOS2	Frequency of Second component for the second cadence.
FOF3	Frequency of First component for the third cadence.

Table 88 show ccm-manager download-tones Output Fields for Dual Tones (continued)

FOS3	Frequency of Second component for the third cadence.
FOF4	Frequency of First component for the fourth cadence.
FOS4	Frequency of Second component for the fourth cadence.
FOT	Frequency of Third component (in Hertz).
FO4	Frequency of Fourth component (in Hertz).
AOT	Amplitude of Third component (from 1 to 65535 = +3 dBm0).
AO4	Amplitude of Fourth component (from 1 to 65535 = +3 dBm0).
RCT1	Number of repeat for the first cadence.
RCT2	Number of repeat for the second cadence.
RCT3	Number of repeat for the third cadence.
RCT4	Number of repeat for the fourth cadence.

Table 89 show ccm-manager download-tones Output Fields for Sequence Tones

Field of Sequence Tone	Description
DR	Direction to PSTN (0) or Packet Network (1).
NF	Number of Frequency (from 1 to 4).
F1C1	Frequency 1 of Cadence 1.
F2C1	Frequency 2 of Cadence 1.
AOF	Amplitude of First component (from 1 to 65535).
AOS	Amplitude of Second component (from 1 to 65535).
C1ONT	Cadence 1 On Time.
C1OFT	Cadence 1 Off Time.
C2ONT	Cadence 2 On Time.
C2OFT	Cadence 2 Off Time.
C3ONT	Cadence 3 On Time.
C3OFT	Cadence 3 Off Time.
C4ONT	Cadence 4 On Time.
C4OFT	Cadence 4 Off Time.
F1C2	Frequency 1 of Cadence 2.
F2C2	Frequency 2 of Cadence 2.
F1C3	Frequency 1 of Cadence 3.
F2C3	Frequency 2 of Cadence 3.
F1C4	Frequency 1 of Cadence 4.
F2C4	Frequency 2 of Cadence 4.

The following is sample output from the **show ccm-manager** command for displaying the status and availability of both the primary and the backup Cisco Unified Communications Manager server:

```
Router# show ccm-manager

MGCP Domain Name: Router2821.cisco.com
Priority        Status                  Host
============================================================
Primary         Registered              10.78.236.222
First Backup    None
Second Backup   None

Current active Call Manager:    10.78.236.222
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            21:48:37 UTC Nov 4 2007 (elapsed time: 00:00:15)
Last MGCP traffic time:         21:48:51 UTC Nov 4 2007 (elapsed time: 00:00:02)
Last failover time:             None
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Not Selected
Last MGCP Fallback start time:  None
Last MGCP Fallback end time:    None
MGCP Download Tones:            Disabled
TFTP retry count to shut Ports: 3


PRI Backhaul Link info:
    Link Protocol:      TCP
    Remote Port Number: 2428
    Remote IP Address:  172.20.71.38
    Current Link State: OPEN
    Statistics:
        Packets recvd:   1
        Recv failures:   0
        Packets xmitted: 3
        Xmit failures:   0
    PRI Ports being backhauled:
       Slot 1, port 1
MGCP Download Tones:             Enabled

Configuration Auto-Download Information
=======================================
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted             : 6
          Download Successful          : 6
          Download Failed              : 0
        Configuration Attempted        : 1
          Configuration Successful     : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
Configuration Error History:
FAX mode: cisco
```

Table 90 describes the significant fields shown in the display.

Table 90 show ccm-manager Field Descriptions

Field	Description
MGCP Domain Name (*system*)	System used in the Internet for translating domain names of network nodes into IP addresses.
Priority	Priority of the Cisco CallManager servers present in the network. Possible priorities are primary, first backup, and second backup.
Status	Current usage of the Cisco Unified Communications Manager server. Values are Registered, Idle, Backup Polling, and Undefined.
Host	Host IP address of the Cisco CallManager server.
Current active Call Manager	IP address of the active Cisco Communications Manager server. This field can be the IP address of any one of the following Cisco Communications Manager servers: Primary, First Backup, and Second Backup.
Backhaul/Redundant link port	Port that the Cisco CallManager server is to use.
Failover Interval	Maximum amount of time that can elapse without the gateway receiving messages from the currently active Cisco Call Manager before the gateway switches to the backup Cisco Call Manager.
Keepalive Interval	Interval following which, if the gateway has not received any messages from the currently active Cisco Communications Manager server within the specified amount of time, the gateway sends a keepalive message to the Cisco Communications Manager server to determine if it is operational.
Last keepalive sent	Time in hours (military format), minutes and seconds at which the last keepalive message was sent.
Last MGCP traffic time	Time in hours (military format), minutes and seconds at which the last MGCP traffic message was sent.
Switchback mode	Displays the switchback mode configuration that determines when the primary Cisco CallManager server is used if it becomes available again while a backup Cisco CallManager server is being used. Values that can appear in this field are Graceful, Immediate, Schedule-time, and Uptime-delay.
MGCP Fallback mode	Displays the MGCP fallback mode configuration. If “Not Selected” displays, then fallback is not configured. If “Enabled/OFF” displays, then fallback is configured but not in effect. If “Enabled/ON” displays, then fallback is configured and in effect.
Last MGCP Fallback start time	Start time stamp in hours (military format), minutes and seconds of the last fallback.
Lasts MGCP Fallback end time	End time stamp in hours (military format), minutes and seconds of the last fallback.
MGCP Download Tones	Displays if the customized tone download is enabled.
TFTP retry count to shut Ports	Number of TFTP download failures allowed before endpoints are shutdown.

The following is sample output from the **show ccm-manager config-download** command showing the status of the SCCP download:

```
Router# show ccm-manager config-download

Configuration Auto-Download Information
=======================================
Current version-id:{4171F93A-D8FC-49D8-B1C4-CE33FA8095BF}
Last config-downloaded:00:00:47
Current state:Waiting for commands
Configuration Download statistics:
        Download Attempted             :6
          Download Successful          :6
          Download Failed              :0
        Configuration Attempted        :1
          Configuration Successful     :1
          Configuration Failed(Parsing):0
          Configuration Failed(config) :0
Last config download command:New Registration

SCCP auto-configuration status
============================================================
Registered with Call Manager: No
Local interface: FastEthernet0/0 (000c.8522.6910)
Current version-id: {D3A886A2-9BC9-41F8-9DB2-0E565CF51E5A}
Current config applied at: 04:44:45 EST Jan 9 2003
Gateway downloads succeeded: 1
Gateway download attempts: 1
Last gateway download attempt:  04:44:45 EST Jan 9 2003
Last successful gateway download: 04:44:45 EST Jan 9 2003
Current TFTP server: 10.2.6.101
Gateway resets: 0
Gateway restarts: 0
Managed endpoints: 6
Endpoint downloads succeeded: 6
Endpoint download attempts: 6
Last endpoint download attempt:  04:44:45 EST Jan 9 2003
Last successful endpoint download: 04:44:45 EST Jan 9 2003
Endpoint resets: 0
Endpoint restarts: 0

Configuration Error History:
sccp ccm CCM-PUB7 identifier 1
end


controller T1 2/0no shut

controller T1 2/0no shut

controller T1 2/0no shut

isdn switch-type primary-ni
end
```

Table 91 describes the significant fields shown in the display.

Table 91 show ccm-manager config-download Field Descriptions

Field	Description
Current state	Current configuration state.
Download Attempted	Number of times the gateway has tried to download the configuration file. The number of successes and failures is displayed.
Configuration Attempted	Number of times the gateway has tried to configure the gateway based on the configuration file. The number of successes and failures is displayed.
Managed endpoints	Number of SSCP-controlled endpoints (analog and BRI phones).
Endpoint downloads succeeded	Number of times the gateway has successfully downloaded the configuration files for SCCP-controlled endpoints.
Endpoint download attempts	Number of times the gateway has tried to download the configuration files for SCCP-controlled endpoints.
Endpoint resets	Number of SCCP gateway resets.
Endpoint restarts	Number of SCCP gateway restarts.
Configuration Error History	Displays SCCP autoconfiguration errors.

The following is sample output from the **show ccm-manager fallback-mgcp** command:

```
Router# show ccm-manager fallback-mgcp

Current active Call Manager:   172.20.71.38
MGCP Fallback mode:            Enabled/OFF
Last MGCP Fallback start time: 00:14:35
Last MGCP Fallback end time:   00:17:25
```

Table 92 displays te mode. Modes are as follows:

Table 92 show ccm-manager fallback-mgcp modes

Field	Description
MGCP Fallback mode	The following are displayed: • Not Selected—Fallback is not configured. • Enabled/OFF—Fallback is configured but not in effect. • Enabled/ON—Fallback is configured and in effect.
Last MGCP Fallback start time	Start time stamp in hh:mm:ss of the last fallback.
Last MGCP Fallback end time	End time stamp in hh:mm:ss of the last fallback.

The following is sample output from the **show ccm-manager music-on-hold** command:

```
Router# show ccm-manager music-on-hold

Current active multicast sessions :1
 Multicast       RTP port    Packets       Call    Codec    Incoming
 Address         number      in/out        id              Interface
=================================================================
172.20.71.38     2428         5/5          99       g711
```

Table 93 describes the significant fields shown in the display.

Table 93 show ccm-manager music-on-hold Field Descriptions

Field	Description
Current active multicast sessions	Number of active calls on hold.
Multicast Address	Valid class D address from which the gateway is getting the RTP streams.
RTP port number	Valid RTP port number on which the gateway receives the RTP packets.
Packets in/out	Number of RTP packets received and sent to the digital signal processor (DSP).
Call id	Call ID of the call that is on hold.
Codec	Codec number.
Incoming Interface	Interface through which the gateway is receiving the RTP stream.

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers, their current status, and their availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show isdn status	Displays the Cisco IOS gateway ISDN interface status.
show mgcp	Displays the MGCP configuration information.

show cdapi

To display the Call Distributor Application Programming Interface (CDAPI), use the **show cdapi** command in privileged EXEC mode.

show cdapi

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.3(4)T	This command was enhanced to display V.120 call types registering with the modem.

Usage Guidelines CDAPI is the internal application programming interface (API) that provides an interface between signaling stacks and applications.

Examples The following is sample output from the **show cdapi** command. The reports are self-explanatory and display the following information:

- Signaling stacks that register with CDAPI
- Applications that register with CDAPI
- Active calls
- Call type of each active call
- Message buffers in use

Enbloc is the mode where all call establishment information is sent in the setup message (opposite of overlap mode, where additional messages are needed to establish the call). Cot is the Continuity Test (COT) subsystem that supports the Continuity Test required by the Signaling System 7 (SS7) network to conduct loopback and tone check testing on the path before a circuit is established.

```
Router# show cdapi

Registered CDAPI Applications/Stacks
====================================

Signaling Stack: ISDN
        Interface: Se6/0:23

Application: TSP CDAPI Application Voice
        Application Type(s) : Voice Data Facility Signaling V110 V120
        Application Level   : Tunnel
        Application Mode    : Enbloc

Application: TSP CDAPI Application COT
```

```
        Application Type(s) : Cot
        Application Level   : Tunnel
        Application Mode    : Enbloc

Application: CSM
        Application Type(s) : Modem V110 V120
        Application Level   : Basic
        Application Mode    : Enbloc

Signaling Stack: XCSP

Application: dialer
        Application Type(s) : Data
        Application Level   : Basic
        Application Mode    : Enbloc

Active CDAPI Calls
==================

        Se7/7:23 Call ID = 0x7717, Call Type = V.120, Application = CSM

CDAPI Message Buffers
=====================

Free Msg Buffers: 320
Free Raw Buffers: 320
Free Large-Raw Buffers: 120
```

Related Commands

Command	Description
debug cdapi	Displays information about the CDAPI.

show ces clock-select

To display the setting of the network clock for the specified port, use the **show ces clock-select** command in privileged EXEC mode.

show ces *slot*/*port* **clock-select**

Syntax Description

slot	Backplane slot number.
/port	Interface port number. The slash must be entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series.

Examples

The following is sample output from this command for slot 1, port 0:

```
Router# show ces 1/0 clock-select

Priority 1 clock source:not configured
Priority 2 clock source:not configured
Priority 3 clock source:ATM1/0 UP
Priority 4 clock source:Local oscillator
Current clock source:ATM1/0, priority:3
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clock-select	Establishes the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module.

show connect

To display configuration information about drop-and-insert connections that have been configured on a router, use the **show connect** command in privileged EXEC mode.

show connect {**all** | **elements** | **name** | **id** | **port** {**T1** | **E1**} *slot/port*}}

Syntax Description

all	Information for all configured connections.
elements	Information for registered hardware or software interworking elements.
name	Information for a connection that has been named by using the **connect** global configuration command. The name you enter is case sensitive and must match the configured name exactly.
id	Information for a connection that you specify by an identification number or range of identification numbers. The router assigns these IDs automatically in the order in which they were created, beginning with 1. The **show connect all** command displays these IDs.
port	Information for a connection that you specify by indicating the type of controller (T1 or E1) and location of the interface.
T1	T1 controller.
E1	E1 controller.
slot/port	Location of the T1 or E1 controller port whose connection status you want to see. Valid values for *slot* and *port* are **0** and **1**. The slash must be entered.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

This command shows drop-and-insert connections on modular access routers that support drop-and-insert. It displays different information in different formats, depending on the keyword that you use.

Examples

The following examples show how the same tabular information appears when you enter different keywords:

```
Router# show connect all

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP

Router# show connect id 1-2

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP

Router# show connect port t1 1/1

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP
```

The following examples show details about specific connections, including the number of time slots in use and the switching elements:

```
Router# show connect id 2

Connection: 2 - Test2
 Current State: ADMIN UP
 Segment 1: -T1 1/0 03
  TDM timeslots in use: 14-18 (5 total)
 Segment 2: -T1 1/1 04
  TDM timeslots in use: 14-18
Internal Switching Elements: VIC TDM Switch

Router# show connect name Test

 Connection: 1 - Test
 Current State: ADMIN UP
 Segment 1: -T1 1/0 01
  TDM timeslots in use: 1-13 (13 total)
 Segment 2: -T1 1/1 02
  TDM timeslots in use: 1-13
Internal Switching Elements: VIC TDM Switch
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
connect	Defines connections between T1 or E1 controller ports for Drop and Insert.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

show controllers rs366

To display information about the RS-366 video interface on the video dialing module (VDM), use the **show controllers rs366** command in privileged EXEC mode.

show controllers rs366 *slot port*

Syntax Description

slot	Slot location of the VDM module. Valid entries are 1 or 2.
port	Port location of the EIA/TIA-366 interface in the VDM module.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples The following example displays information about the RS-366 controller:

```
Router# show controllers rs366 0 1

RS366:driver is initialized in slot 1, port 0:

STATUS STATE LSR  LCR  ICSR EXT  T1     T2     T3     T4     T5
0x02   0x01  0x00 0x50 0xE0 0x00 5000   5000   5000   20000  10000
Dial string:
121C
```

Table 94 describes significant fields shown in this output.

Table 94 show controllers rs366 Field Descriptions

Field	Description
STATUS	Last interrupt status.
STATE	Current state of the state machine.
LSR	Line status register of the VDM.
LCR	Line control register of the VDM.
ICSR	Interrupt control and status register of the VDM.
EXT	Extended register of the VDM.
T1 through T5	Timeouts 1 through 5 of the watchdog timer, in milliseconds.
Dial string	Most recently dialed number collected by the driver. 0xC at the end of the string indicates the EON (end of number) character.

show controllers timeslots

To display the channel-associated signaling (CAS) and ISDN PRI state in detail, use the **show controllers timeslots** command in privileged EXEC mode.

show controllers t1/e1 *controller-number* **timeslots** *timeslot-range*

Syntax Description

tl/e1 *controller-number*	Controller number of CAS or ISDN PRI time slot. Range is from 0 to 7.
timeslots *timeslot-range*	Timeslot. E1 range is from 1 to 31. T1 range is from 1 to 24.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The **timeslots** keyword was added.
12.1(5)T	This command was implemented on the Cisco AS5400.

Usage Guidelines

Use this command to display the CAS and ISDN PRI channel state in detail. The command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Use the **show controllers e1** or **show controllers t1** command to display statistics about the E1 or T1 links.

Examples

The following example shows that the CAS state is enabled on the Cisco AS5300 with a T1 PRI card:

```
Router# show controllers timeslots

T1 1 is up:
Loopback: NONE
DS0  Type       Modem    <->     Service       Channel       Rx          Tx
                                 State         State        A B C D     A B C D
-------------------------------------------------------------------------------
  1    cas-modem   1       in     insvc       connected    1  1  1  1    1  1  1  1
  2    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  3    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  4    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  5    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  6    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  7    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  8    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  9    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  10   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  11   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  12   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
```

```
 13   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 14   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 15   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 16   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 17   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 18   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 19   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 20   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 21   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 22   unused
 23   unused
 24   unused
```

The following example shows that the ISDN PRI state is enabled on the Cisco AS5300 with a T1 PRI card:

```
T1 2 is up:
Loopback: NONE
DS0 Type         Modem    <->  Service   Channel     Rx        Tx
                                State     State       A B C D   A B C D
--------------------------------------------------------------------------------
 1  pri          -        -    insvc     idle
 2  pri          -        -    insvc     idle
 3  pri          -        -    insvc     idle
 4  pri          -        -    insvc     idle
 5  pri          -        -    insvc     idle
 6  pri          -        -    insvc     idle
 7  pri          -        -    insvc     idle
 8  pri          -        -    insvc     idle
 9  pri          -        -    insvc     idle
10  pri          -        -    insvc     idle
11  pri          -        -    insvc     idle
12  pri          -        -    insvc     idle
13  pri          -        -    insvc     idle
14  pri          -        -    insvc     idle
15  pri          -        -    insvc     idle
16  pri          -        -    insvc     idle
17  pri          -        -    insvc     idle
18  pri          -        -    insvc     idle
19  pri          -        -    insvc     idle
20  pri          -        -    insvc     idle
21  pri-modem    2        in   insvc     busy
22  pri-modem    1        out  insvc     busy
23  pri-digi     -        in   insvc     busy
24  pri-sig      -        -    outofsvc  reserved
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show controllers e1	Displays information about E1 links.
show controllers t1	Displays information about T1 links.

show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command in privileged EXEC mode.

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5)XQ	This command was introduced on the Cisco 1750.

Usage Guidelines This command displays interface status information that is specific to voice-related hardware, such as the registers of the TDM switch, the host port interface of the digital signal processor (DSP), and the DSP firmware versions. The information displayed is generally useful only for diagnostic tasks performed by technical support.

Examples The following is sample output from this command:

```
Router# show controllers voice

EPIC Switch registers:
STDA 0xFF STDB 0xFF SARA 0xAD SARB 0xFF SAXA 0xFF SAXB 0x0 STCR 0x3F
MFAIR 0x3F
STAR 0x65 OMDR 0xE2 VNSR 0x0 PMOD 0x4C PBNR 0xFF POFD 0xF0 POFU 0x18
PCSR 0x1 PICM 0x0 CMD1 0xA0 CMD2 0x70 CBNR 0xFF CTAR 0x2 CBSR 0x20 CSCR
0x0

DSP 0 Host Port Interface:
HPI Control Register 0x202
InterfaceStatus 0x2A MaxMessageSize 0x80
RxRingBufferSize 0x6 TxRingBufferSize 0x9
pInsertRx 0x4 pRemoveRx 0x4 pInsertTx 0x6 pRemoveTx 0x6

Rx Message 0:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 0000 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0

Rx Message 1:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 0000 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

```
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB

Rx Message 2:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 0000 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0

Rx Message 3:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 0000 C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1

Rx Message 4:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 0000 DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

Rx Message 5:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 0000 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

Tx Message 0:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 003C DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

Tx Message 1:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 003C 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

Tx Message 2:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 003C 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0

Tx Message 3:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 003C 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

```
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB

Tx Message 4:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 003C 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0

Tx Message 5:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 003C C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1

Tx Message 6:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDA 3E48 3A84 0000 003C E75F 4E46 403F 4147
0020:   5174 D5C7 BFBC BCBE C5D4 6C4C 3F3B 3939 3D46 5BDA
0040:   C5BC B7B6 B8BD C8E9 4F3F 3834 3437 3D4C EEC8 BBB5
0060:   B2B3 B8BF D35A 4138 3331 3339 435F CEBD B6B1 B1B4
0080:   BBC9 7C48 3B34 3131 363D 4FDE

Tx Message 7:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC5 5F08 9131 0000 003C 66DE 66EB 67EE FE6E
0020:   F7E7 6B68 E068 EE6A DF5C DF62 EDF1 6FF2 7A78 67DC
0040:   5EDF 62E7 64E6 66E0 7071 EA69 F86E E260 DE5D E665
0060:   EB75 F0FB 6DE9 64E4 69E3 66EA 67E9 6DF9 F177 EC6E
0080:   EB6E F876 F875 7D6E E966 E05D

Tx Message 8:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDB 3E48 3AD4 0000 003C C2B9 B3B1 B3B8 C2DC
0020:   523F 3733 3235 3C49 72CB BDB7 B4B5 B8BF CF67 483C
0040:   3836 373C 455C DAC6 BDB9 B9BB C0CC EE54 453E 3C3C
0060:   3F47 56F1 D1C7 C1BF C0C6 CEE1 6651 4A46 4648 4D59
0080:   70E3 D6CF CDCE D2D9 E67E 675E

Bootloader 1.8, Appn 3.1
Application firmware 3.1.8, Built by claux on Thu Jun 17 11:00:05 1999

VIC Interface Foreign Exchange Station 0/0, DSP instance (0x19543C0)
Singalling channel num 128 Signalling proxy 0x0 Signaling dsp 0x19543C0
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 1
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
650070 bytes output, 4976 frames output, 0 output errors, 0 output
underrun
0 unaligned frames

VIC Interface Foreign Exchange Station 0/1, DSP instance (0x1954604)
Singalling channel num 129 Signalling proxy 0x0 Signaling dsp 0x1954604
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 2
received 0 packets, 0 bytes, 0 gaint packets
```

```
0 drops, 0 no buffers, 0 input errors 0 input overruns
393976 bytes output, 3982 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
```

Field descriptions are hardware-dependent and are meant for use by trained technical support.

Related Commands

Command	Description
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show interface dspfarm	Displays hardware information including DRAM, SRAM, and the revision-level information on the line card.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.

show crm

To display the carrier call capacities statistics, use the **show crm** command in privileged EXEC mode.

show crm

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Both the **show trunk group** command and the **show crm** command display values for the maximum number of calls. These values originate from different configuration procedures:

- In the **show trunk group** command, the Max Calls value originates from the **max-calls** command in the trunk group configuration.
- In the **show crm** command, Max calls indicates the maximum number of available channels after the carrier ID or trunk group label is assigned to an interface using the **trunk-group** (interface) command.

Examples The following example illustrates the carrier call capacities statistics:

```
Router# show crm

Carrier:1411
    Max calls:4
    Max Voice (in) :      4    Cur Voice (in) :      0
    Max Voice (out):      4    Cur Voice (out):      0
    Max Data (in)  :      4    Cur Data (in)  :      0
    Max Data (out) :      4    Cur Data (out) :      0

Trunk Group Label: 100
    Max calls:6
    Max Voice (in) :      6    Cur Voice (in) :      0
    Max Voice (out):      6    Cur Voice (out):      0
    Max Data (in)  :      6    Cur Data (in)  :      0
    Max Data (out) :      6    Cur Data (out) :      0
```

Table 95 describes the fields shown in this output, in alphabetical order.

Table 95 show crm Field Descriptions

Field	Description
Carrier	ID of the carrier that handles the calls.
Cur Data (in)	Current number of incoming data calls that are handled by the carrier or trunk group.
Cur Data (out)	Current number of outgoing data calls that are handled by the carrier or trunk group.
Cur Voice (in)	Current number of incoming voice calls that are handled by the carrier or trunk group.
Cur Voice (out)	Current number of outgoing voice calls that are handled by the carrier or trunk group.
Max Calls	Maximum number of calls that are handled by the carrier or trunk group.
Max Data (in)	Maximum number of incoming data calls that are handled by the carrier or trunk group.
Max Data (out)	Maximum number of outgoing data calls that are handled by the carrier or trunk group.
Max Voice (in)	Maximum number of incoming voice calls that are handled by the carrier or trunk group.
Max Voice (out)	Maximum number of outgoing voice calls that are handled by the carrier or trunk group.
Trunk Group Label	Label of the trunk group that handles the calls.

Related Commands

Command	Description
carrier-id (dial peer)	Specifies the carrier associated with VoIP calls.
max-calls	Specifies the maximum number of calls handled by a trunk group.
show trunk group	Displays the configuration parameters for one or more trunk groups.
trunk-group (interface)	Assigns an interface to a trunk group.
trunk-group-label (dial peer)	Specifies the trunk group associated with VoIP calls.

show csm

To display the call switching module (CSM) statistics for a particular digital signal processor (DSP) channel, all DSP channels, or a specific modem or DSP channel, use the **show csm** command in privileged EXEC mode.

Cisco AS5300 Universal Access Server

show csm {**call-rate** [**table**] | **call-resource** | **modem** [*slot*/*port* | **group** *modem-group-number*] | **signaling-channel**}

Cisco AS5400Series Router

show csm {**call rate** [**table**] | **call-resource** | **modem** [*slot*/*port* | **group** *modem-group-number*] | **signaling-channel** | **voice** [*slot*/*port*]}

Syntax Description

call-rate	Displays the incoming and outgoing call switching rate.
table	(Optional) Displays the incoming and outgoing call switching rate in the form of numerical table.
call-resource	Displays statistics about the CSM call resource.
modem	Displays CSM call statistics for modems.
slot/*port*	(Optional) Location (and thereby identity) of a specific modem.
group	(Optional) Displays modem group information.
modem-group-number	(Optional) Location of a particular dial peer. Range: 1 to 32767.
signaling-channel	Displays CSM signaling channel Information.
voice	Displays CSM call statistics for DSP channels.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(3)T	This command was modified. Port-specific values for the Cisco AS5300 were added.
12.0(7)T	This command was modified. Port-specific values for the Cisco AS5800 were added.

Usage Guidelines

This command shows the information related to CSM, which includes the DSP channel, the start time of the call, the end time of the call, and the channel on the controller used by the call.

Use the **show csm modem** command to display the CSM call statistics for a specific modem, for a group of modems, or for all modems. If a *slot*/*port* argument is specified, then CSM call statistics are displayed for the specified modem. If the *modem-group-number* argument is specified, the CSM call statistics for all of the modems associated with that modem group are displayed. If no keyword is specified, CSM call statistics for all modems on the Cisco AS5300 universal access server are displayed.

Use the **show csm voice** command to display CSM statistics for a particular DSP channel. If the *slot/dspm/dsp/dsp-channel* or *shelf/slot/port* argument is specified, the CSM call statistics for calls using the identified DSP channel are displayed. If no argument is specified, all CSM call statistics for all DSP channels are displayed.

Examples

The following is sample output from the **show csm** command for the Cisco AS5300 universal access server:

```
Router# show csm voice 2/4/4/0

 slot 2, dspm 4, dsp 4, dsp channel 0,
 slot 2, port 56, tone, device_status(0x0002): VDEV_STATUS_ACTIVE_CALL.

csm_state(0x0406)=CSM_OC6_CONNECTED, csm_event_proc=0x600E2678, current call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u0, c22), tdm_chnl=TDM_DSP_STREAM(s2, c27)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0xA003, bchan_num=22
csm_event=CSM_EVENT_ISDN_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=3
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0
call_duration_started=00:06:53, call_duration_ended=00:00:00, total_call_duration=00:00:44
The calling party phone number = 408
The called party phone number  = 5271086
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_dynamic_busy_rbs_timeslot
= 0, total_static_busy_rbs_timeslot = 0,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 21, total_busy_isdn_channels = 0,total_auto_busy_isdn_channels
= 0,
min_free_device_threshold = 0
```

Table 96 describes the significant fields shown in the display.

Table 96 show csm voice Field Descriptions

Field	Description
slot	Slot where the VFC resides.
dsp	DSP through which this call is established.
slot/port	Logical port number for the device. This is equivalent to the DSP channel number. The port number is derived as follows: • (max_number_of_dsp_channels per dspm=12) * the dspm # (0-based) + • (max_number_of_dsp_channels per dsp=2) * the dsp # (0-based) + the dsp channel number (0-based).

Table 96 show csm voice Field Descriptions (continued)

Field	Description
tone	Which signaling tone is being used (DTMF, MF, R2). This only applies to CAS calls. Possible values are as follows: • mf • dtmf • r2-compelled • r2-semi-compelled • r2-non-compelled
device_status	Status of the device. Possible values are as follows: • VDEV_STATUS_UNLOCKED—Device is unlocked (meaning that it is available for new calls). • VDEV_STATUS_ACTIVE_WDT—Device is allocated for a call and the watchdog timer is set to time the connection response from the central office. • VDEV_STATUS_ACTIVE_CALL—Device is engaged in an active, connected call. • VDEV_STATUS_BUSYOUT_REQ—Device is requested to busyout; does not apply to voice devices. • VDEV_STATUS_BAD—Device is marked as bad and not usable for processing calls. • VDEV_STATUS_BACK2BACK_TEST—Modem is performing back-to-back testing (for modem calls only). • VDEV_STATUS_RESET—Modem needs to be reset (for modem only). • VDEV_STATUS_DOWNLOAD_FILE—Modem is downloading a file (for modem only). • VDEV_STATUS_DOWNLOAD_FAIL—Modem has failed during downloading a file (for modem only). • VDEV_STATUS_SHUTDOWN—Modem is not powered up (for modem only). • VDEV_STATUS_BUSY—Modem is busy (for modem only). • VDEV_STATUS_DOWNLOAD_REQ—Modem is requesting connection (for modem only).

Table 96 show csm voice Field Descriptions (continued)

Field	Description
csm_state	CSM call state of the current call (PRI line) associated with this device. Possible values are as follows: • CSM_IDLE_STATE—Device is idle. • CSM_IC_STATE—A device has been assigned to an incoming call. • CSM_IC1_COLLECT_ADDR_INFO—A device has been selected to perform ANI/DNIS address collection for this call. ANI/DNIS address information collection is in progress. The ANI/DNIS is used to decide whether the call should be processed by a modem or a voice DSP. • CSM_IC2_RINGING—The device assigned to this incoming call has been told to get ready for the call. • CSM_IC3_WAIT_FOR_SWITCH_OVER—A new device is selected to take over this incoming call from the device collecting the ANI/DNIS address information. • CSM_IC4_WAIT_FOR_CARRIER—This call is waiting for the CONNECT message from the carrier. • CSM_IC5_CONNECTED—This incoming call is connected to the central office. • CSM_IC6_DISCONNECTING—This incoming call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process. • CSM_OC_STATE —An outgoing call is initiated. • CSM_OC1_REQUEST_DIGIT—The device is requesting the first digit for the dial-out number. • CSM_OC2_COLLECT_1ST_DIGIT—The first digit for the dial-out number has been collected. • CSM_OC3_COLLECT_ALL_DIGIT—All the digits for the dial-out number have been collected. • CSM_OC4_DIALING—This call is waiting for a dsx0 (B channel) to be available for dialing out. • CSM_OC5_WAIT_FOR_CARRIER—This (outgoing) call is waiting for the central office to connect. • CSM_OC6_CONNECTED—This (outgoing) call is connected. • CSM_OC7_BUSY_ERROR—A busy tone has been sent to the device (for VoIP call, no busy tone is sent; just a DISCONNECT INDICATION message is sent to the VTSP module), and this call is waiting for a DISCONNECT message from the VTSP module (or ONHOOK message from the modem) to complete the disconnect process. • CSM_OC8_DISCONNECTING—The central office has disconnected this (outgoing) call, and the call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process.

Table 96 show csm voice Field Descriptions (continued)

Field	Description
csm_state: invalid_event_count	Number of invalid events received by the CSM state machine.
wdt_timeout_count	Number of times the watchdog timer is activated for this call.
wdt_timestamp_started	Whether the watchdog timer is activated for this call.
wait_for_dialing	Whether this (outgoing) call is waiting for a free digit collector to become available to dial out the outgoing digits.
wait_for_bchan	Whether this (outgoing) call is waiting for a B channel to send the call out on.
pri_chnl	Which type of TDM stream is used for the PRI connection. For PRI and CAS calls, it is always TDM_PRI_STREAM.
tdm_chnl	Which type of TDM stream is used for the connection to the device used to process this call. In the case of a VoIP call, this is always set to TDM_DSP_STREAM.
dchan_idb_start_index	First index to use when searching for the next IDB of a free D channel.
dchan_idb_index	Index of the currently available IDB of a free D channel.
csm_event	Event just passed to the CSM state machine.
cause	Event cause.
ring_no_answer	Number of times a call failed because there was no response.
ic_failure	Number of failed incoming calls.
ic_complete	Number of successful incoming calls.
dial_failure	Number of times a connection failed because there was no dial tone.
oc_failure	Number of failed outgoing calls.
oc_complete	Number of successful outgoing calls.
oc_busy	Number of outgoing calls whose connection failed because there was a busy signal.
oc_no_dial_tone	Number of outgoing calls whose connection failed because there was no dial tone.
oc_dial_timeout	Number of outgoing calls whose connection failed because the timeout value was exceeded.
call_duration_started	Start of this call.
call_duration_ended	End of this call.
total_call_duration	Duration of this call.
The calling party phone number	Calling party number as given to CSM by ISDN.
The called party phone number	Called party number as given to CSM by ISDN.
total_free_rbs_time slot	Total number of free RBS (CAS) time slots available for the whole system.
total_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been busied-out. This includes both dynamically and statically busied out RBS time slots.

Table 96 show csm voice Field Descriptions (continued)

Field	Description
total_dynamic_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been dynamically busied out.
total_static_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been statically busied out (that is, they are busied out using the CLI command).
total_free_isdn_channels	Total number of free ISDN channels.
total_busy_isdn_channels	Total number of busy ISDN channels.
total_auto_busy_isdn_channels	Total number of ISDN channels that are automatically busied out.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show num-exp	Displays how number expansions are configured.
show voice port	Displays configuration information about a specific voice port.

show csm call

To view the call switching module (CSM) call statistics, use the **show csm call** command in privileged EXEC mode

show csm call {**failed** | **rate** | **total**}

Syntax Description

failed	CSM call fail/reject rate for the last 60 seconds, 60 minutes, and 72 hours.
rate	CSM call rate for the last 60 seconds, 60 minutes, and 72 hours.
total	Total number of CSM calls for the last 60 seconds, 60 minutes, and 72 hours.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines Use this command to understand CSM call volume.

Examples The following examples show the CSM call statistics for the last 60 seconds:

```
Router# show csm call rate


  15
  14
  13
  12
  11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
         CSM call switching rate per second (last 60 seconds)
         # = calls entering the module per second
```

```
Router# show csm call failed


  15
  14
  13
  12
  11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
         CSM call fail/reject rate per second (last 60 seconds)
           # = calls failing per second


Router# sh csm call total


1344
1244
1144
1044
 944
 844
 744
 644
 544
 444
 344
 244
 144
  44
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
                  CSM total calls (last 60 seconds)
                       # = number of calls
```

Field descriptions should be self-explanatory.

show debug condition

To display the debugging filters that have been enabled for VoiceXML applications, ATM-enabled interfaces, or Frame Relay interfaces, use the **show debug condition** command in privileged EXEC mode.

show debug condition

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S and was enhanced to include debugging for ATM-enabled and Frame Relay-enabled interfaces.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(9)T	This command was enhanced to include debugging for ATM-enabled and Frame Relay-enabled interfaces.

Usage Guidelines

This command displays the debugging filter conditions that have been set for VoiceXML applications by using the **debug condition application voice** command.

Examples

The following is sample output from this command when it is used with the VoiceXML application:

```
Router# show debug condition

Condition 1: application voice vmail (1 flags triggered)
       Flags: vmail
Condition 2: application voice myapp1 (1 flags triggered)
       Flags: myapp1
```

The following is sample output from this command when an ATM interface is being debugged:

```
Router# show debug condition

Condition 1: atm-vc 0/56784 AT2/0 (0 flags triggered)
Condition 2: atm-vc 255/45546 AT2/0 (0 flags triggered)
Condition 3: atm-vc 0/266 AT6/0 (1 flags triggered)
```

Table 97 describes the significant fields shown in the display.

Table 97 show debug condition Field Descriptions

Field	Description
Condition 1	Sequential number identifying the filter condition that was set for the specified command.
Flags	Name of the voice application for which the condition was set.
at2/0	Interface number of the ATM interface that has the debug condition applied.
atm-vc 0/56784	Virtual channel identifier (VCI). Alternatively, virtual path identifier/virtual channel identifier (VCI/VPI) pair.

Related Commands

Command	Description
debug condition application voice	Filters out debugging messages for all VoiceXML applications except the specified application.
debug http client	Displays debugging messages for the HTTP client.
debug vxml	Displays debugging messages for VoiceXML features.

show dial-peer

To display the dial plan mapping table for protocol peers, use the **show dial-peer** command in privileged EXEC mode.

show dial-peer {**carrier** | **cor** | **trunk-group-label**}

Syntax Description

carrier	Displays carrier ID configuration details of the peer protocol.
cor	Displays restriction settings class details.
trunk-group-label	Displays trunk group label configuration details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17)SX	This command was introduced.
12.4(22)T	This command was modified in a release earlier than Cisco IOS Release 12.4(22)T. The **carrier** and **trunk-group-label** keywords were added.

Usage Guidelines

Use this command to display the dial plan mapping table for protocol peers along with the available keywords.

Examples

The following sample output from the **show dial-peer** command displays restriction settings class details. The fields are self-explanatory.

```
Router# show dial-peer cor

Class of Restriction

name: class1
```

show dial-peer video

To display configuration information for video dial peers, use the **show dial-peer video** command in privileged EXEC mode.

show dial-peer video [*number*] [**summary**]

Syntax Description

number	(Optional) A specific video dial peer. Output displays information about that dial peer.
summary	(Optional) Output displays a one-line summary of each video dial peer.

Defaults

If both the *name* argument and **summary** keyword are omitted, command output displays detailed information about all video dial peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to display the configuration for all video dial peers configured for a router. To show configuration information for only one specific dial peer, use the *number* argument to identify the dial peer.

Examples

The following sample output displays detailed information about all configured video dial peers:

```
Router# show dial-peer video

Video Dial-Peer 1
      type = videocodec, destination-pattern = 111
      port signal = 1/0, port media = Serial1
      nsap = 47.0091810000000050E201B101.00107B09C6F2.C8
Video Dial-Peer 2
      type = videoatm,   destination-pattern = 222
      session-target = ATM0 svc nsap 47.0091810000000050E201B101.00E01E92ADC2.C8
Video Dial-Peer 3
      type = videoatm,   destination-pattern = 333
      session-target = ATM0 pvc 70/70
```

show dial-peer voice

To display information for voice dial peers, use the **show dial-peer voice** command in user EXEC or privileged EXEC mode.

show dial-peer voice [*number* | **busy-trigger-counter** | **summary** | **voip system**]

Syntax Description

number	(Optional) A specific voice dial peer. The output displays detailed information about that dial peer.
busy-trigger-counter	(Optional) Displays the busy trigger call count on the VoIP dial peer.
summary	(Optional) Displays a short summary of each voice dial peer.
voip system	(Optional) Displays information about the VoIP dial peer.

Command Default

If both the *number* argument and **summary** keyword are omitted, the output displays detailed information about all voice dial peers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was modified. The **summary** keyword was added for the Cisco MC3810.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was implemented for VoFR on the Cisco 7200 series.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(2)XN	This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager 3.2 and implemented on the Cisco IAD2420. The command was enhanced to display configuration information for bandwidth, video codec, and rtp payload-type for H.263+ and H.264 video codec.

Release	Modification
12.4(22)T	This command was modified. This command was enhanced to display the current configuration state of the history-info header. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for outgoing calls.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The output was enhanced to display information about the bind at the dial-peer level and to display the connection status of Foreign Exchange Office (FXO) ports.

Usage Guidelines

Use this command to display the configuration for all VoIP and POTS dial peers configured for a gateway. To display configuration information for only one specific dial peer, use the *number* argument. To display summary information for all dial peers, use the **summary** keyword.

Examples

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Router# show dial-peer voice 100

VoiceEncapPeer3201
peer type = voice, information type = video,
description = `',
tag = 3201, destination-pattern = `86001',
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
source carrier-id = `',target carrier-id = `',
source trunk-group-label = `',target trunk-group-label = `',
numbering Type = `unknown'
group = 3201, Admin state is up, Operation state is up,
Outbound state is up,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
URI classes:
        Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
        incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
type = pots, prefix = `',
forward-digits 4
session-target = `', voice-port = `2/0:23',
direct-inward-dial = enabled,
digit_strip = enabled,
```

```
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size =  20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
        maximum = 384 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
        inbound = `', outbound = `1'
Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

The following is sample output from this command for a VoIP dial peer:

```
Router# show dial-peer voice 101

VoiceOverIpPeer101
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 1234, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
allow watch = FALSE
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
rtp-ssrc mux = system
source carrier-id = `', target carrier-id = `',
source trunk-group-label = `',  target trunk-group-label = `',
numbering Type = `unknown'
group = 1234, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem transport = system,
URI classes:
Incoming (Request) =
Incoming (Via) =
Incoming (To) =
Incoming (From) =
Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = `',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef
```

```
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
lmr_tone=0, nte_tone=0
h263+=118, h264=119
G726r16 using static payload
G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
video codec = None
voice class codec = `'
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rel1xx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number = system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
```

```
voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number  = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.

When there is no Dial-peer level bind -
voice class sip bind control = system,
voice class sip bind media = system,
```

The following is sample output from the **show dial-peer voice summary** command that shows connected FXO port 0/2/0 (the last entry) has OUT STAT set to “up,” which indicates that the POTS dial peer can be used for an outgoing call. If this port is disconnected, the status changes in the output so that the OUT STAT field reports “down,” and the POTS dial peer cannot be used for an outgoing call.

Note Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports—any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to “up” for FXO port 0/2/0:

```
000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0,
changed state to operational status up due to cable reconnection
```

```
Router# show dial-peer voice summary

dial-peer hunt 0
                AD                                      PRE PASS                OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE
39275- voip  up   up             .T                 0  syst ipv4:172.18.108.26
82
```

```
8880    pots  up    up              8880              0                      up    2/0/0
8881    pots  up    up              8881              0                      up    2/0/1
8882    pots  up    up              8882              0                      up    2/0/2
8883    pots  up    up              8883              0                      up    2/0/3
8884    pots  up    up              8884              0                      up    2/0/4
8885    pots  up    up              8885              0                      up    2/0/5
8886    pots  up    up              8886              0                      up    2/0/6
8887    pots  up    up              8887              0                      up    2/0/7
88888-  pots  up    up                                0                    down   0/3/0:23
888
65033-  pots  up    up              6503352           0                      up    0/2/0
52
```

Table 94 describes the significant fields shown in the displays, in alphabetical order.

Table 94 show dial-peer voice Field Descriptions

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
bandwidth maximum/minimum	The maximum and minimum bandwidth, in Kb/s.
Charged Units	Total number of charging units that have applied to this peer since system startup, in hundredths of a second.
CLID Restriction	Indicates if Calling Line ID (CLID) restriction is enabled.
CLID Network Number	Displays the network number sent as CLID, if configured.
CLID Second Number sent	Displays whether a second calling number is stripped from the call setup.
CLID Override RDNIS	Indicates whether the CLID is overridden by the redirecting number.
codec	Default voice codec rate of speech.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls, in hundredths of a second.
connections/maximum	Indicates the maximum number of call connections per peer.
Destination	Indicates the voice class that is used to match the destination URL.
destination-pattern	Destination pattern (telephone number) for this peer.
digit_strip	Indicates if digit stripping is enabled.
direct-inward-dial	Indicates if direct inward dial is enabled.
disconnect-cause	Indicates the disconnect cause code to be used when an incoming call is blocked.
dnis-map	Name of the dialed-number identification service (DNIS) map.
DTMF Relay	Indicates if dual-tone multifrequency (DTMF) relay is enabled.
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.

Table 94 show dial-peer voice Field Descriptions (continued)

Field	Description
fax rate	Fax transmission rate configured for this peer.
forward-digits	Indicates the destination digits to be forwarded of this peer.
group	Group number associated with this peer.
huntstop	Indicates whether dial-peer hunting is turned on, by the **huntstop** command, for this dial peer.
Icpif	Configured Impairment/Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer.
in bound application associated	Interactive voice response (IVR) application that is configured to handle inbound calls to this dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming call blocking	Indicates the incoming call blocking setup of this peer.
incoming called-number	Indicates the incoming called number if it has been set.
incoming COR list	Indicates the level of Class of Restrictions for incoming calls of this peer.
Incomplete Calls	Indicates the number of outgoing disconnected calls with the user busy (17), no user response (18), or no answer (19) cause code.
information type	Information type for this call (voice, fax, video).
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the system uptime when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
numbering Type	Indicates the numbering type for a peer call leg.
Operation state	Operational state of this peer.
outgoing COR list	Indicates the level of Class of Restrictions for outgoing calls of this peer.
outgoing LPCOR	Setting of the **lpcor outgoing** command.
out bound application associated	The voice application that is configured to handle outbound calls from this dial peer. Outbound calls are handed off to the named application.
Outbound state	Indicates the current outbound status of a POTS peer.
payload size	Indicates the size (in bytes) of the payload of the fax rate or codec setup.
payload type	NSE payload type.
peer type	Dial peer type (voice, data).
permission	Configured permission level for this peer.
Poor QOV Trap	Indicates if poor quality of voice trap messages is enabled.

Table 94 show dial-peer voice Field Descriptions (continued)

Field	Description
preemption level	Indicates the call preemption level of this peer.
prefix	Indicates dialed digits prefix of this peer.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
register E.164 number with H.323 GK and/or SIP Registrar	Indicates the "register e.164" option of this peer.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
session-protocol	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.
source carrier-id	Indicates the source carrier ID of this peer that will be used to match the source carrier ID of an incoming call.
source trunk-group label	Indicates the source trunk group label of this peer that can be used to match the source trunk group label of an incoming call.
Successful Calls	Number of completed calls to this peer.
supported-language	Indicates the list of supported languages of this peer.
tag	Unique dial peer ID number.
target carrier-id	Indicates the target carrier ID of this peer that will be used to match the target carrier ID for an outgoing call.
target-trunkgroup-label	Indicates the target trunk group label of this peer that can be used to match the target trunk group label of an outgoing call.
Time elapsed since last clearing of voice call statistics	Elapsed time between the current time and the time when the **clear dial-peer voice** command was executed.
Translation profile (Incoming)	Indicates the translation profile for incoming calls.
Translation profile (Outgoing)	Indicates the translation profile for outgoing calls.
translation-profile	Indicates the number translation profile of this peer.
type	Indicates the peer encapsulation type (pots, voip, vofr, voatm or mmoip).
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.
voice class called-number inbound/outbound	Indicates the voice-class called number inbound or outbound setup of this peer.
voice class sip history-info	Indicates the configuration state of the history-info header. If the history-info header is not configured for the dial peer, this field is set to system. If the history-info header is enabled on this dial peer, this field is set to enable. If the history-info header is disabled on this dial peer, this field is set to disable.

Table 94 show dial-peer voice Field Descriptions (continued)

Field	Description
voice class sip bind	Indicates the configuration state of the bind address. If the bind is configured for the global, this field is sent to system. If the bind address is enabled on this dial peer, this field is set to enabled.
voice-port	Indicates the voice interface setting of this POTS peer.

The following is sample output from this command with the **summary** keyword:

```
Router# show dial-peer voice summary

dial-peer hunt 0
                                                        PASS
  TAG TYPE   ADMIN OPER PREFIX   DEST-PATTERN     PREF THRU SESS-TARGET    PORT
  100 pots   up    up                             0
  101 voip   up    up            5550112          0   syst ipv4:10.10.1.1
  102 voip   up    up            5550134          0   syst ipv4:10.10.1.1
   99 voip   up    down                           0   syst
   33 pots   up    down                           0
```

Table 95 describes the significant fields shown in the display.

Table 95 show dial-peer voice summary Field Descriptions

Field	Description
dial-peer hunt	Hunt group selection order that is defined for the dial peer by the **dial-peer hunt** command.
TAG	Unique identifier assigned to the dial peer when it was created.
TYPE	Type of dial peer (mmoip, pots, voatm, vofr, or voip).
ADMIN	Whether the administrative state is up or down.
OPER	Whether the operational state is up or down.
PREFIX	Prefix that is configured in the dial peer by the **prefix** command.
DEST-PATTERN	Destination pattern that is configured in the dial peer by the **destination-pattern** command.
PREF	Hunt group preference that is configured in the dial peer by the **preference** command.
PASS THRU	Modem pass-through method that is configured in the dial peer by the **modem passthrough** command.
SESS-TARGET	Destination that is configured in the dial peer by the **session target** command.
PORT	Router voice port that is configured for the dial peer. Valid only for POTS dial peers.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call history table.

Command	Description
show dialplan incall number	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is reached when a specific telephone number is dialed.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show dialplan dialpeer

To display the outbound dial peers that are matched to an incoming dial peer based on the class of restriction (COR) criteria and the dialed number, use the **show dialplan dialpeer** command in privileged EXEC mode.

show dialplan dialpeer *incoming-dialpeer-tag* **number** *number* [**timeout**]

Syntax Description

incoming-dialpeer-tag	The dial peer COR identifier used to determine the matching outbound dial peer.
number *number*	The dialed number used in conjunction with the COR identifier to determine the matching outbound dial peer.
timeout	(Optional) Allows matching for variable-length destination patterns.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5800 access servers.
12.2(11)T	This command was implemented on the Cisco 1751 and Cisco 3700 series routers and on Cisco AS5300 access servers.

Usage Guidelines

Use this command as a troubleshooting tool to determine which outbound dial peer is matched for an incoming call, based on the COR criteria and dialed number specified in the command line. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

Note For actual voice calls coming into the router, the incoming corlist of a specified inbound dial peer and the outgoing called number will be used to match the outbound dial peer.

Examples

The following sample output shows an incoming call with a dialed number of 19001111 and meeting the COR criteria as part of dial peer 300 with incoming COR-list has been matched to an outbound dial peer with IP address 1.8.50.7:

```
Router# show dialplan dialpeer 300 number 1900111

VoiceOverIpPeer900
        information type = voice,
        description = `',
        tag = 900, destination-pattern = `1900',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 900, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
```

```
        modem passthrough = system,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:to900
        type = voip, session-target = `ipv4:1.8.50.7',
        technology prefix:
        settle-call = disabled
        ...
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 19001111   Digits: 4
Target: ipv4:1.8.50.7
```

Table 96 describes the significant fields shown in the display.

Table 96 show dialplan command Field Descriptions

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the calling number entered.
VoiceOverIpPeer	Dial peer associated with the calling number entered.
peer type	Type of this dial peer (voice or data).
information type	Information type for this dial peer (voice or data).
description	Any additional information for this dial peer entered using the **description** dial peer command.
tag	Unique number identifying the dial peer.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
CLID restriction	Indicates the Caller ID restriction (if any) configured for this dial peer.
CLID Network Number	Indicates the originating network of the Caller ID source.
CLID Second Number sent	Indicates the digits in the second number (if any) forwarded for this dial peer.
source carrier-id	VoIP or POTS source carrier identifier.
source trunk-group-label	VoIP or POTS source trunk group identifier.
numbering Type	Identifies the numbering scheme employed for this dial peer.
group	Dial peer group in which this dial peer is a member.
Admin state	Administrative state of this dial peer.

Table 96 show dialplan command Field Descriptions (continued)

Field	Description
Operation state	Operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
connections/maximum	Number of actual and maximum allowable connections associated with this dial peer.
DTMF Relay	Whether the **dtmf-relay** command is enabled or disabled for this dial peer.
URI classes: Incoming (Request)	URI voice class used for matching dial peer to Request-URI in an incoming SIP Invite message.
URI classes: Incoming (To)	URI voice class used for matching dial peer to the To header in an incoming SIP Invite message.
URI classes: Incoming (From)	URI voice class used for matching dial peer to the From header in an incoming SIP Invite message.
URI classes: Destination	URI voice class used to match the dial peer to the destination URI for an outgoing call.
modem transport	Transport method configured for modem calls. The default is system, which means that the value configured globally is used.
huntstop	Whether the **huntstop** command is enabled or disabled for this dial peer.
in bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
dnis-map	Name of the dialed-number identification service (DNIS) map that is configured in the dial peer with the **dnis-map** command.
permission	Configured permission level for this dial peer.
incoming COR list	Class of restriction (COR) criteria associated when matching an incoming dial peer.
outgoing COR list	COR criteria used to determine the appropriate outbound dial peer.
Translation profile (Incoming)	Incoming translation criteria applied to this dial peer.
Translation profile (Outgoing)	Translation criteria applied to this dial peer when matching an outbound dial peer.
incoming call blocking	Indicates whether or not incoming call blocking has been applied for this dial peer.
translation-profile	The predefined translation profile associated with this dial peer.
disconnect-cause	Encoded network cause associated with the last call.
voice-port	Voice port through which calls come into this dial peer.
type	Type of dial peer (POTS or VoIP).
prefix	Prefix number that is added to the front of the dial string before it is forwarded to the telephony device.

Table 96 show dialplan command Field Descriptions (continued)

Field	Description
forward-digits	Which digits are forwarded to the telephony interface as configured using the **forward-digits** command.
session-target	Configured session target (IP address or host name) for this dial peer.
direct-inward-dial	Whether the **direct-inward-dial** command is enabled or disabled for this dial peer.
digit_strip	Whether digit stripping is enabled or disabled in the dial peer. Enabled is the default.
register E.164 number with GK	Indicates whether or not the dial peer has been configured to register its full E.164-format number with the local gatekeeper.
fax rate	The transmission speed configured for fax calls. The default is system, which means that the value configured globally is used.
payload size	The size (in bytes) for a fax transmission payload.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
req-qos	Configured requested quality of service for calls for this dial peer.
acc-qos	Lowest acceptable quality of service configured for calls for this dial peer.
codec	Voice codec configured for this dial peer. Default is G.729 (8 kbps).
Expect factor	User-requested expectation factor of voice quality for calls through this dial peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by this dial peer.
VAD	Indicates whether or not voice activation detection (VAD) is enabled for this dial peer.
voice class sip url	URL format (SIP or TEL) used for SIP calls to this dial peer, as configured with the **voice-class sip url** command. The default is system, which means that the value configured globally with the **url** command in voice service VoIP SIP mode is used.
voice class sip rel1xx	Indicates whether or not reliable provisional responses are supported, as configured with the **voice-class sip rel1xx** command. The default is system, which means that the value configured globally with the **rel1xx** command in voice service VoIP SIP mode is used.
voice class perm tag	Voice class for a trunk that is assigned to this dial peer with the **voice-class permanent** command.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this dial peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this dial peer since system startup.

Table 96 show dialplan command Field Descriptions (continued)

Field	Description
Incomplete Calls	Number of incomplete calls to this dial peer since system startup.
Accepted Calls	Number of calls from this dial peer accepted since system startup.
Refused Calls	Number of calls from this dial peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Digits	Number of digits in this destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan incall

To display which incoming POTS dial peer is matched for a specific calling number or voice port, use the **show dialplan incall number** command in privileged EXEC mode.

show dialplan incall *voice-port* **number** *calling-number* [**timeout**]

Syntax Description

voice-port	Voice port location. The syntax of this argument is platform-specific. For information on the syntax for a particular platform, see the **voice-port** command.
calling-number	E.164 Calling number or ANI of the incoming voice call.
timeout	(Optional) Allows matching for variable-length destination patterns.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the **timeout** keyword was added.

Usage Guidelines

Use this command as a troubleshooting tool to determine which POTS dial peer is matched for an incoming call, for the selected calling number and voice port. The router attempts to match these items in the order listed:

1. Calling number with answer-address configured in dial peer
2. Calling number with destination-pattern configured in dial peer
3. Voice port with voice port configured in dial peer

The router first attempts to match a dial peer based on the calling number (ANI). If the router is unable to match a dial peer based on the calling number, it matches the call to a POTS dial peer based on the selected voice interface. If more than one dial peer uses the same voice port, the router selects the first matching dial peer. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.

Note For actual voice calls coming into the router, the router attempts to match the called number (the dialed number identification service [DNIS] number) with the incoming called-number configured in a dial peer. The router, however, does not consider the called number when using the **show dialplan incall number** command.

Examples

The following sample output shows that an incoming call from interface 1/0/0:D with a calling number of 12345 is matched to POTS dial peer 10:

```
Router# show dialplan incall 1/0/0:D number 12345

Macro Exp.: 12345

VoiceEncapPeer10
        information type = voice,
        tag = 10, destination-pattern = `123..',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 10, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `1/0/0:D',
        direct-inward-dial = disabled,
        digit_strip = enabled,

        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,

        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 12345   Digits: 3
Target:
```

The following sample output shows that, if no dial peer has a destination pattern or answer address that matches the calling number of 888, the incoming call is matched to POTS dial peer 99, because the call comes in on voice port 1/0/1:D, which is the voice port configured for this dial peer:

```
Router# show dialplan incall 1/0/1:D number 888

Macro Exp.: 888

VoiceEncapPeer99
        information type = voice,
        tag = 99, destination-pattern = `99...',
        answer-address = `', preference=1,
        numbering Type = `national'
        group = 99, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `5',
```

```
        forward-digits 4
        session-target = `', voice-port = `1/0/1:D',
        direct-inward-dial = enabled,
        digit_strip = enabled,
register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Note Table 96 describes the significant fields shown in the display.

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan incall uri

To display which dial peer is matched for a specific uniform resource identifier (URI) in an incoming voice call, use the **show dialplan incall uri** command in privileged EXEC mode.

H.323 Session Protocol

show dialplan incall uri h323 {**called** | **calling**} *uri*

SIP Session Protocol

show dialplan incall uri sip {**from** | **request** | **to**} *uri*

Syntax Description

called	Voice class that is configured in dial peers with the **incoming uri called** command.
calling	Voice class that is configured in dial peers with the **incoming uri calling c**ommand.
from	Voice class that is configured in dial peers with the **incoming uri from** command.
request	Voice class that is configured in dial peers with the **incoming uri request** command.
to	Voice class that is configured in dial peers with the **incoming uri to** command.
uri	URI of the incoming call.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command for troubleshooting to determine which dial peer is matched for an incoming call, based on the selected URI and the specified field in the call message.
- To set the URI format for matching calls, use the **voice class uri** command. To set the URI voice class in the inbound dial peer, use the **incoming uri** command.

Examples

The following is sample output from this command for a SIP URI:

```
Router# show dialplan incall uri sip from sip:5551234

Inbound VoIP dialpeer matching based on SIP URI's

VoiceOverIpPeer10
        peer type = voice, information type = voice,
        description = `',
        tag = 10, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 10, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
        URI classes:
            Incoming (Request) =
            Incoming (To) =
            Incoming (From) = 101
            Destination =
        huntstop = disabled,
        in bound application associated: 'get_headers_tcl'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        type = voip, session-target = `',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
        session-protocol = sipv2, session-transport = system, req-qos = best-ef
        acc-qos = best-effort,
        RTP dynamic payload type values: NTE = 101
        Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
               CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
        RTP comfort noise payload type = 19
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax-relay ecm enable
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout Mode is set to default,
        Initial 60 ms, Max 300 ms
        Playout-delay Minimum mode is set to default, value 40 ms
        Fax nominal 300 ms
        Max Redirects = 1, signaling-type = ext-signal,
        VAD = enabled, Poor QOV Trap = disabled,
        Source Interface = NONE
        voice class sip url = system,
        voice class sip rel1xx = system,
        voice class perm tag = `'
```

```
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

The following is sample output from this command for a TEL URI:

```
Router# show dialplan incall uri h323 called tel:1234567

 Inbound VoIP dialpeer matching based on H323 URI's

VoiceOverIpPeer25
        peer type = voice, information type = voice,
        description = `',
        tag = 25, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 25, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
        URI classes:
            Incoming (Called) = 103
            Incoming (Calling) =
            Destination =
        huntstop = disabled,
        in bound application associated: 'callme'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        type = voip, session-target = `ipv4:10.10.1.1',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
        session-protocol = cisco, session-transport = system, req-qos = best-ef
        acc-qos = best-effort,
        RTP dynamic payload type values: NTE = 101
        Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
               CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
        RTP comfort noise payload type = 19
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax-relay ecm enable
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout Mode is set to default,
```

```
        Initial 60 ms, Max 300 ms
        Playout-delay Minimum mode is set to default, value 40 ms
        Fax nominal 300 ms
        Max Redirects = 1, signaling-type = ext-signal,
        VAD = enabled, Poor QOV Trap = disabled,
        Source Interface = NONE
        voice class sip url = system,
        voice class sip rel1xx = system,
        voice class perm tag = `'
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Table 97 describes significant fields in the displays.

Table 97 show dialplan incall uri Field Descriptions

Field	Description
VoiceOverIpPeer	Dial peer associated with the calling number entered.
information type	Information type for this call; for example, voice or fax.
tag	Unique number that identifies the dial peer.
destination-pattern	Destination pattern (called number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
Admin state	Administrative state of this dial peer.
Operation state	Operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
DTMF Relay	Whether the **dtmf-relay** command is enabled or disabled for this dial peer.
URI classes: Incoming (Request)	URI voice class used for matching dial peer to Request-URI in an incoming SIP Invite message.
URI classes: Incoming (To)	URI voice class used for matching dial peer to the To header in an incoming SIP Invite message.
URI classes: Incoming (From)	URI voice class used for matching dial peer to the From header in an incoming SIP Invite message.
URI classes: Destination	URI voice class used to match the dial peer to the destination URI for an outgoing call.
huntstop	Whether the **huntstop** command is enabled or disabled for this dial peer.
in bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.

Table 97 show dialplan incall uri Field Descriptions (continued)

Field	Description
dnis-map	Name of the dialed-number identification service (DNIS) map that is configured in the dial peer with the **dnis-map** command.
permission	Configured permission level for this peer.
type	Type of dial peer (POTS or VoIP).
session-target	Configured session target (IP address or host name) for this dial peer.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
req-qos	Configured requested quality of service for calls for this dial peer.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
codec	Voice codec configured for this dial peer. Default is G.729 (8 kbps).
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by a dial peer.
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.
voice class sip url	URL format (SIP or TEL) used for SIP calls to this dial peer, as configured with the **voice-class sip url** command. The default is system, which means that the value configured globally with the **url** command in voice service VoIP SIP mode is used.
voice class sip rel1xx	Whether reliable provisional responses are supported, as configured with the **voice-class sip rel1xx** command. The default is system, which means that the value configured globally with the **rel1xx** command in voice service VoIP SIP mode is used.
voice class perm tag	Voice class for a trunk that is assigned to this dial peer with the **voice-class permanent** command.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls from this peer accepted since system startup.
Refused Calls	Number of calls from this peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
session protocol	Specifies the session protocol in the dial peer for calls between the local and remote router.
show dial-peer voice	Displays detailed and summary information about voice dial peers.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

show dialplan in-carrier

To display which incoming VoIP or POTS dial peer is matched for a specific source carrier or voice port, use the **show dialplan in-carrier** command in privileged EXEC mode.

show dialplan in-carrier carrier-id [**voip** | **pots**]

Syntax Description

carrier-id	VoIP or POTS source carrier identifier.
voip	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
pots	(Optional) Allows you to limit the search criteria to only POTS dial peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

Usage Guidelines

Use this command as a troubleshooting tool to determine which VoIP or POTS dial peer is matched for an incoming call, based on the carrier identifier specified in the command line. Use the **voip** or **pots** keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

Examples

The following sample output shows a VoIP or POTS dial peer being matched to another POTS dial peer based on its carrier identifier, “aaa”:

```
Router# show dialplan in-carrier aaa pots

 Inbound pots dialpeer Matching based on source carrier-id

VoiceEncapPeer7777
        information type = voice,
        description = `',
        tag = 7777, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `aaa',      target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 7777, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated:'DEFAULT'
        out bound application associated:''
        dnis-map =
        permission :both
```

```
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
voice-port = `'
        type = pots, prefix = `',
        forward-digits default
        session-target = `', up,
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE
        fax rate = system,   payload size =  20 bytes

        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:   Digits:0
Target:
```

Note Table 96 describes the significant fields shown in the display.

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan in-trunk-group-label

To display which incoming VoIP or POTS dial peer is matched for a specific trunk group label, use the **show dialplan in-trunk-group-label** command in privileged EXEC mode.

show dialplan in-trunk-group-label *trunk-group-label* [**pots** | **voip**]

Syntax Description

trunk-group-label	VoIP or POTS source trunk group identifier.
voip	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
pots	(Optional) Allows you to limit the search criteria to only POTS dial peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

Usage Guidelines

Use this command to determine which VoIP or POTS dial peer is matched for an incoming call, based on the identifier of the source trunk group. The router attempts to match these items in the order listed. Use the **voip** or **pots** keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

Examples

The following sample output shows an inbound VoIP or POTS dial peer being matched to an outbound POTS dial peer based on the trunk group label “NYtrunk”:

```
Router# show dialplan in-trunk-group-label NYtrunk pots

 Inbound pots dialpeer Matching based on source trunk-group-label

VoiceEncapPeer2003
        information type = voice,
        description = `',
        tag = 2003, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `NYtrunk',   target trunk-group-label = `',
        numbering Type = `unknown'
        group = 2003, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated:'debit-card'
        out bound application associated:''
        dnis-map =
        permission :both
```

```
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
voice-port = `'
        type = pots, prefix = `',
        forward-digits default
        session-target = `', up,
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE
        fax rate = system,   payload size =  20 bytes

        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:   Digits:0
Target:
```

Note Table 96 describes the significant fields shown in the display.

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan number

To display which outgoing dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in privileged EXEC mode.

show dialplan number *dial-string* [**carrier** *identifier*] [**fax | huntstop | voice**] [**timeout**]

Syntax Description

dial-string	Particular destination pattern (E.164 telephone number).
carrier	(Optional) Indicates that you wish to base your search for applicable dial peers on the source carrier identifier.
identifier	(Optional) Source carrier identifier to accompany the **carrier** keyword.
fax	(Optional) Fax information type.
huntstop	(Optional) Terminates further dial-peer hunting upon encountering the first dial-string match.
timeout	(Optional) Allows matching for variable-length destination patterns.
voice	(Optional) Voice information type.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(1)	The **huntstop** keyword was added.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the **timeout** keyword was added.
12.2(11)T	The **carrier**, **fax**, and **voice** keywords were added.

Usage Guidelines

Use this command to test whether the dial plan configuration is valid and working as expected. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.

Examples

The following is sample output from this command using a destination pattern of 1001:

```
Router# show dialplan number 1001

Macro Exp.: 1001

VoiceEncapPeer1003
        information type = voice,
        tag = 1003, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1003, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = enabled,
```

```
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `1/1',
        direct-inward-dial = disabled,
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1004
        information type = voice,
        tag = 1004, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1004, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1002
        information type = voice,
        tag = 1002, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1002, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1001
        information type = voice,
        tag = 1001, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1001, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:
```

The following is sample output from this command using a destination pattern of 1001 and the **huntstop** keyword:

```
Router# show dialplan number 1001 huntstop

 Macro Exp.: 1001

 VoiceEncapPeer1003
        information type = voice,
        tag = 1003, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1003, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = enabled,
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `1/1',
        direct-inward-dial = disabled,
        Connect Time = 0, Charged Units = 0,
```

```
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:
```

Note Table 96 describes the significant fields shown in the display.

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.

show dialplan uri

To display which outbound dial peer is matched for a specific destination uniform resource identifier (URI), use the **show dialplan uri** command in privileged EXEC mode.

show dialplan uri *uri*

Syntax Description

uri	Destination Session Initiation Protocol (SIP) or telephone (TEL) URI for the outgoing call.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command for troubleshooting to determine which dial peer is matched for an outgoing call, based on the selected URI.
- To set the URI format used to match calls, use the **voice class uri** command. To set the URI voice class in the outbound dial peer, use the **destination uri** command.

Examples

The following is sample output from this command:

```
Router# show dialplan uri sip:123456

 Outbound dialpeer matching based on destination URI

VoiceOverIpPeer99
        peer type = voice, information type = voice,
        description = `',
        tag = 99, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 99, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
```

```
        URI classes:
            Incoming (Request) =
            Incoming (To) =
            Incoming (From) =
            Destination = 100
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        type = voip, session-target = `',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
        session-protocol = sipv2, session-transport = system, req-qos = best-ef
        acc-qos = best-effort,
        RTP dynamic payload type values: NTE = 101
        Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
               CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
        RTP comfort noise payload type = 19
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax-relay ecm enable
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout Mode is set to default,
        Initial 60 ms, Max 300 ms
        Playout-delay Minimum mode is set to default, value 40 ms
        Fax nominal 300 ms
        Max Redirects = 1, signaling-type = ext-signal,
        VAD = enabled, Poor QOV Trap = disabled,
        Source Interface = NONE
        voice class sip url = system,
        voice class sip rel1xx = system,
        voice class perm tag = `'
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Table 97 on page 2017 describes significant fields in the display.

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.

Command	Description
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

show dn-numbers

To display directory number information of Call Manager Express (CME), use the **show dn-numbers** command in user EXEC or privileged EXEC mode.

show dn-numbers

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#))

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Examples

The following is sample output from the **show dn-numbers** command:

```
Router# show dn-numbers

 Directory numbers
 Entry          name                          number
 1             user1                          0
 10            user2                          7890
 3             user3                          1234
 4             user4                          890
 12            user5                          5676
 11            user6                          987

 ephone directory numbers

 DN             name                           number
 2              user7                          1000
 4              user10                         34567
 6              user11                         1234567891
 10             user12                         1234567

sip phone numbers

 DN             name                           number
 1              user13                         10000
 8              user14                         87953893
 9              user15                         Not Configured
```

Table 98 describes the significant fields shown in the display.

Table 98 show dn-numbers Field Descriptions

Field	Description
DN	Directory number.
name	Name of the connection.
number	Telephone number.

show dspfarm

To display digital signal processor (DSP) farm service information such as operational status and DSP resource allocation for transcoding and conferencing, use the **show dspfarm** command in user EXEC or privileged EXEC mode.

show dspfarm [**all** | **dsp** {**active** | **all** | **idle** | **stats** *bridge-id* [**sample** *seconds*]} | **profile** [*profile-id*] | **sessions** [*session-id*] | **video** {**conference** | **statistics** | **transcode**}]

Cisco ASR 1000 Series Router

show dspfarm {**all** | **dsp** {**active** | **all** | **idle** | **stats** *bridge-id* [**sample** *seconds*]} | **profile** [*profile-identifier*]}

Syntax Description

all	(Optional) Displays all global information about the DSP farm service.
dsp	(Optional) Displays DSP information about the DSP farm service.
active	Displays active DSP information about the DSP farm service.
all	Displays all DSP information about the DSP farm service.
idle	Displays idle DSP information about the DSP farm service.
stats	Displays DSP statistics about the DSP farm service.
bridge-id	Displays the DSP statistics for a call bridge the specified bridge ID.
sample	(Optional) Displays statistics of the specified sample interval.
seconds	(Optional) The DSP sample interval time, in seconds.
profile	(Optional) Displays profiles about the DSP farm service.
profile-id	(Optional) The profile ID about the DSP farm service.
sessions	(Optional) Displays sessions and connections about the DSP farm service.
session-id	(Optional) The session identifier to be displayed for the DSP farm service.
video	(Optional) Displays information on video resources.
conference	(Optional) Displays the DSP information, such as the codecs, video bridge channel, and transmit (tx) and receive (rx) packets that are used for each participant in a conference and is grouped by conference sessions.
statistics	(Optional) Displays the DSP statistics of the call bridge.
transcode	(Optional) Displays the DSP status and statistics for the transcoding call.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.4(15)T	The **stats**, **sample**, **sessions**, and **profile** keywords were added. The *bridge-id*, *profile-id*, *seconds*, and *session-id* arguments were added.

Release	Modification
Cisco IOS XE Release 3.2S	This command was implemented on the Cisco ASR 1000 Series Router.
15.1(4)M	This command was modified. The **video**, **conference**, **statistics**, and **transcode** keywords were added.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Cisco ASR 1000 Series Router

The show dspfarm command is used to view the DSP farm service information such as operational status and DSP resource allocation for transcoding.

Note The **session** keyword and *session-id* argument is not supported on Cisco ASR 1000 Series Router.

Examples

The following is sample output from several forms of the **show dspfarm** command. The fields are self explanatory.

```
Router# show dspfarm

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 0
RTP Timeout: 600

Router# show dspfarm all

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 2
RTP Timeout: 1200
Connection average duration: 3600, Connection check interval 600
Codec G729 VAD: ENABLED

Total number of active session(s) 0, and connection(s) 0

SLOT  DSP   CHNL  STATUS USE   TYPE   SESS-ID   CONN-ID   PKTS-RXED PKTS-TXED

1     3     1     UP     FREE  conf   -         -         -         -
1     3     2     UP     FREE  conf   -         -         -         -
1     3     3     UP     FREE  conf   -         -         -         -
1     3     4     UP     FREE  conf   -         -         -         -
1     3     5     UP     FREE  conf   -         -         -         -
1     3     6     UP     FREE  conf   -         -         -         -
1     4     1     UP     FREE  conf   -         -         -         -
1     4     2     UP     FREE  conf   -         -         -         -
1     4     3     UP     FREE  conf   -         -         -         -
1     4     4     UP     FREE  conf   -         -         -         -
1     4     5     UP     FREE  conf   -         -         -         -
1     4     6     UP     FREE  conf   -         -         -         -
1     5     1     UP     FREE  xcode  -         -         -         -
1     5     2     UP     FREE  xcode  -         -         -         -
1     5     3     UP     FREE  xcode  -         -         -         -
```

```
1     5     4     UP     FREE  xcode  -         -         -         -
1     5     5     UP     FREE  xcode  -         -         -         -
1     5     6     UP     FREE  xcode  -         -         -         -
1     5     7     UP     FREE  xcode  -         -         -         -
1     5     8     UP     FREE  xcode  -         -         -         -

Total number of DSPFARM DSP channel(s) 20

Router# show dspfarm dsp all

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 2
RTP Timeout: 1200
Connection average duration: 3600, Connection check interval 600
Codec G729 VAD: ENABLED

Total number of active session(s) 0, and connection(s) 0

SLOT  DSP  CHNL  STATUS  USE   TYPE   SESS-ID  CONN-ID  PKTS-RXED  PKTS-TXED

1     3    1     UP      FREE  conf   -        -        -          -
1     3    2     UP      FREE  conf   -        -        -          -
1     3    3     UP      FREE  conf   -        -        -          -
1     3    4     UP      FREE  conf   -        -        -          -
1     3    5     UP      FREE  conf   -        -        -          -
1     3    6     UP      FREE  conf   -        -        -          -
1     4    1     UP      FREE  conf   -        -        -          -
1     4    2     UP      FREE  conf   -        -        -          -
1     4    3     UP      FREE  conf   -        -        -          -
1     4    4     UP      FREE  conf   -        -        -          -
1     4    5     UP      FREE  conf   -        -        -          -
1     4    6     UP      FREE  conf   -        -        -          -
1     5    1     UP      FREE  xcode  -        -        -          -
1     5    2     UP      FREE  xcode  -        -        -          -
1     5    3     UP      FREE  xcode  -        -        -          -
1     5    4     UP      FREE  xcode  -        -        -          -
1     5    5     UP      FREE  xcode  -        -        -          -
1     5    6     UP      FREE  xcode  -        -        -          -
1     5    7     UP      FREE  xcode  -        -        -          -
1     5    8     UP      FREE  xcode  -        -        -          -

Total number of DSPFARM DSP channel(s) 20

Router# show dspfarm sessions

sess_id  conn_id  stype  mode      codec  pkt  ripaddr      rport  sport
4        145      xcode  sendrecv  g711a  20   10.10.10.19  19460  21284
4        161      xcode  sendrecv  g729   10   10.10.10.28  19414  20382
5        177      xcode  sendrecv  g711u  20   10.10.10.17  18290  21170
5        193      xcode  sendrecv  g729b  10   10.10.10.18  19150  18968
```

The following sample output displays dspfarm profiles for video conferencing and video transcoding.

```
Router# show dspfarm profile

 Profile ID = 1, Service = VIDEO CONFERENCING, Resource ID = 2
 Video Conference Type : HOMOGENEOUS, Layout : disabled
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : DOWN
 Profile Operation State : DOWN
 Application : SCCP   Status : NOT ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : NONE
```

```
 Number of Resource Configured : 1
 Number of Resource Available : 0
 Maximum conference participants : 16
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729r8, Maximum Packetization Period : 60
 Codec : g729br8, Maximum Packetization Period : 60
 Video Codec Configuration:
 Codec : h263
   Resolution : cif
     Frame rate:30, Min bitrate:320kbps, Max bitrate:320kbps
     Payload protocol : rfc-2190, Extension : annex-none


 Profile ID = 2, Service = VIDEO CONFERENCING, Resource ID = 3
 Video Conference Type : HETEROGENEOUS, Layout : disabled
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE IN PROGRESS
 Application : SCCP   Status : ASSOCIATION IN PROGRESS
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 1
 Number of Resource Available : 1
 Maximum conference participants : 4
 Maximum video ports : 4
 Codec Configuration: num_of_codecs:6
 Codec : g729br8, Maximum Packetization Period : 60
 Codec : g729r8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g711ulaw, Maximum Packetization Period : 30
 Video Codec Configuration:
 Codec : h264
   Resolution : qcif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
   Resolution : cif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
 Codec : h263
   Resolution : qcif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
   Resolution : cif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps

Dspfarm Profile Configuration
Profile ID = 3, Service =Universal TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : DOWN
 Profile Operation State : DOWN
 Application : SCCP   Status : NOT ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : NONE
 Number of Resource Configured : 0
 Number of Resource Available : 0
 Codec Configuration: num_of_codecs:4
 Codec : g711ulaw, Maximum Packetization Period : 30
```

```
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
```

The following sample output displays DSP information for video conferences.

```
Router# show dspfarm video conference


 VIDEO CONFERENCE SESSION: slot 0 dsp 3 channel_id 1 rsc_id 8 profile_id 101
 conferee_id 1  name_num:  62783363
         audio_codec g711u     pkt_size 160  bridge_id 1
         dsp_txed_pkts 25993     dsp_rxed_pkts 25888
 conferee_id 1  name_num:  62783363
         video_codec H264_VGA  rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 960  annex 0x40
         cluster_id 0  bridge_id 2         layout_id 0
         dsp_txed_pkts 59230     dsp_rxed_pkts 63019
 conferee_id 2  name_num:  62783365
         audio_codec g711u     pkt_size 160  bridge_id 3
         dsp_txed_pkts 21682     dsp_rxed_pkts 21598
 conferee_id 2  name_num:  62783365
         video_codec H264_4CIF rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 960  annex 0x40
         cluster_id 1  bridge_id 4         layout_id 0
         dsp_txed_pkts 49488     dsp_rxed_pkts 78510
 conferee_id 3  name_num:  3004
         audio_codec g711u     pkt_size 160  bridge_id 5
         dsp_txed_pkts 12130     dsp_rxed_pkts 12067
 conferee_id 3  name_num:  3004
         video_codec H264_CIF  rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 704  annex 0x40
         cluster_id 2  bridge_id 6         layout_id 0
         dsp_txed_pkts 20354     dsp_rxed_pkts 25702
 conferee_id 4  name_num: LifeSize LifeSize
         audio_codec g711u     pkt_size 160  bridge_id 7
         dsp_txed_pkts 1751      dsp_rxed_pkts 1672
 conferee_id 4  name_num: LifeSize LifeSize
         video_codec H264_4CIF rfc_number RFC3984 payload rx: 96   tx:96
         framerate 30 bitrate(k) 1100 annex 0x40
         cluster_id 1  bridge_id 8         layout_id 0
         dsp_txed_pkts 3558      dsp_rxed_pkts 3569

 cluster_id 0  video_codec H264_VGA  rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 1000, annex 0x40
 decoder_id 1  slot 0  dsp 13 codec h264 vga           cluster_id 0
 encoder_id 1  slot 0  dsp 10 codec h264 vga           cluster_id 0

 cluster_id 1  video_codec H264_4CIF rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 1000, annex 0x40
 decoder_id 1  slot 0  dsp 2  codec h264 4cif          cluster_id 1
 encoder_id 1  slot 0  dsp 7  codec h264 4cif          cluster_id 1

 cluster_id 2  video_codec H264_CIF  rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 704 , annex 0x40
 decoder_id 1  slot 0  dsp 15 codec h264 cif           cluster_id 2
 encoder_id 1  slot 0  dsp 14 codec h264 cif           cluster_id 2

Total number of DSPFARM DSP channel(s) 1
```

The following sample output displays the statistics for a call that uses video transcoding.

```
Router# show dspfarm dsp stats

Gathering total stats...

Video Statistics for bridge_id=3 call_id=2

 Video Decoder Statistics:
  Slot=0  DSP_Id=8  Decoder_Id=1
  CallDuration=268  Codec=1  ProfileId=0x0  LevelId=0
  PicWidth=352  PicHeight=288  FrameRate=30  Bitrate=360000
  NumMacroBlocksConcealed=0  NumFramesConcealed=0
  NumPackets=13269  NumBytesConsumed=12096254
  NumBadHeaderPackets=0  NumOutOfSyncPackets=24
  NumBufferOverflow=0
 Video Encoder Statistics:
  Slot=0  DSP_Id=2  Encoder_Id=1
  Duration=268  Codec=1  ProfileId=0x0  LevelId=0
  PicWidth=176  PicHeight=144  FrameRate=30  Bitrate=704000
  InstantBitrate=440000  NumPackets=17571  NumBytesGenerated=14830996
```

The following sample output displays the statistics for a video conference.

```
Router# show dspfarm dsp stats

Gathering total stats...

Video Statistics for bridge_id=3 call_id=4

 Video Conferee Status - ConfereeID=1
  ContributionState=0x1  IngressMute=0  EgressMute=0
  DtmfRtpPlt=0  ClusterId=1  StreamDir=3
  PayloadType=0x6161  TxSSRC=0x1F3C  RtpProtocol=2
  CodecType=2  Annex=0x0  PicWidth=352  PicHeight=288
  FrameRate=30  Bitrate(x100)=3760

 Video Conferee Statistics - ConfereeID=1
  TotalRxPackets=5076  TotalRxBytes=3957126
  TotalTxPackets=3829  TotalTxBytes=3429797
  TotalDroppedPackets=3  CurDroppedPackets=0
  TotalOutOfOrderPackets=0  CurOutOfOrderPackets=0
  MaxObservedJitter=0  CurObservedJitter=0
  MaxObservedDelay=0  CurObservedDelay=0
  MaxOutOfSyncDelay=0  CurOutOfSyncDelay=0
  ActualFrameRate=0  ActualBitrate(x100)=2017
  FastVideoUpdateRate=0  TotalDuration=135

 Video Conference Status:
  ServiceType=0  MuteAllStatus=0
  CurSpeakerConfereeId=1  LastSpeakerConfereeId=3  NewSpeakerConfereeId=0
  ConfereeIdBitMap=0x07

 Video Conference Statistics:
  NumActiveChans=3  NumMaxChans=1
  TotalRxPackets=42589  TotalRxBytes=29979147
  TotalTxPackets=12361  TotalTxBytes=10003701
  TotalDroppedPackets=3  CurDroppedPackets=0
  TotalOutOfOrderPackets=0  CurOutOfOrderPackets=0
  MaxObservedJitter=0  CurObservedJitter=0
  MaxObservedDelay=0  CurObservedDelay=0
MaxOutOfSyncDelay=0  CurOutOfSyncDelay=0
```

The following is sample output of the **show dspfarm all** command on Cisco ASR 1000 Series Router.

```
Router# show dspfarm all
Dspfarm Profile Configuration

 Profile ID = 1, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SBC   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resources Configured : 588
 Number of Resources Out of Service : 0
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60


SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID

5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
```

The following is sample output of the **show dspfarm dsp idle** command providing idle dsp information on Cisco ASR 1000 Series Router.

```
Router# show dspfarm dsp idle

SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID

5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
```

The following is sample output of the **show dspfarm profile 1** command providing DSP Farm profile configuration details such as application association, number of resources configured, Codecs added, and maximum number of sessions for profile 1 on Cisco ASR 1000 Series Router.

```
Router# show dspfarm profile 1
Dspfarm Profile Configuration

 Profile ID = 1, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SBC   Status : ASSOCIATED
```

```
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resources Configured : 588
 Number of Resources Out of Service : 0
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
Router#show dspfarm profile ?
  <1-65535>  Profile ID
  |          Output modifiers
  <cr>
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.

show dspfarm profile

To display configured digital signal processor (DSP) farm profile information for a selected Cisco CallManager group, use the **show dspfarm profile** command in privileged EXEC mode.

show dspfarm profile [*profile-identifier*]

Syntax Description

profile-identifier	(Optional) Number that uniquely identifies a profile. Range is from 1 to 65535. There is no default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show dspfarm profile** command to verify that the association between Skinny Client Control Protocol (SCCP) Cisco Unified CallManager and the DSP farm profiles match your organizational plan.

The output of the **show dspfarm profile** command differs depending on the services configured in the profile.

Examples

The following is sample output from the **show dspfarm profile** command:

```
Router# show dspfarm profile

Dspfarm Profile Configuration

 Profile ID = 6, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 4
 Number of Resource Available : 4
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729br8, Maximum Packetization Period : 60

 RSVP : ENABLED

 TRP : FW-TRAVERSAL ENABLED

Dspfarm Profile Configuration

 Profile ID = 27, Service = CONFERENCING, Resource ID = 2
```

```
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 6
 Number of Resource Available : 6
 Codec Configuration
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60

Dspfarm Profile Configuration

 Profile ID = 34, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : UP
 Number of Resource Configured : 2
 Number of Resource Available : 2
 Hardware Configured Resources : 1
 Hardware Available Resources : 1
 Software Resources : 1
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 TRP : FW-TRAVERSAL ENABLED
```

Table 99 describes the significant fields shown in the display.

Table 99 show dspfarm profile Field Descriptions

Field	Description
Profile ID	Displays the profile ID number.
Service	Displays the service that is associated with the profile.
Resource ID	Displays the ID number that the profile is associated with in the Cisco CallManager register.
Profile Description	Displays the description of the profile.
Profile Service Mode	The status of the profile service. It can be either Secure or Non Secure.
Profile Admin State	Displays the status of the profile. If the Profile Admin State is DOWN, use the **no shutdown** command in DSP farm profile configuration mode.

Table 99 show dspfarm profile Field Descriptions (continued)

Field	Description
Profile Operation State	Displays the status of the DSP farm profiles registration process with the Cisco CallManager. Status options are as follows: • ACTIVE—The profile is registered with the Cisco Unified CallManager. • ACTIVE IN PROGRESS—The profile is still registering with the Cisco Unified CallManager. Wait for the profile to finish registering. • DOWN—The profile is not registering with the Cisco Unified CallManager. Check the connectivity between the DSP farm gateway and the Cisco Unified CallManager. • DOWN IN PROGRESS—The profile is deregistering from the Cisco Unified CallManager and deallocating the DSP resources. • RESOURCE ALLOCATED—The DSP resources for this profile are allocated or reserved.
Application	Displays the routing protocol used.
Number of Resource Configured	Maximum number of sessions that are supported by a profile.
Number of Resource Available	Total number of resources that are configurable.
Hardware Configured Resources	Number of sessions configured in the profile.
Hardware Available Resources	Number of sessions available for this profile.
Software Resources	Number of software sessions configured for this profile (applicable only to MTP profiles).
Codec Configuration	Lists the codecs that are configured. **Note** Media Termination Point (MTP) profile supports only one codec per profile.
RSVP	Resource Reservation Protocol (RSVP) support for this profile.
TRP	Displays whether firewall traversal is enabled for Trusted Relay Point.

Related Commands

Command	Description
dsp services dspfarm	Configures DSP farm services for a specified voice card.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show media resource status	Displays the current media resource status.

show dsp-group

To display digital signal processor (DSP) group information including both voice and video information, use the **show dsp-group** command in user EXEC or privileged EXEC mode.

show dsp-group {**all** | **slot** *slot-number* | **video** [**all** | **slot** *slot-number*] | **voice** [**all** | **slot** *slot-number*]}

Syntax Description

all	Displays DSP information for all DSP group.
slot	Displays DSP information for the specified slot.
slot-number	Slot used in the DSP group.
video	Displays information on video resources.
voice	Displays information on voice resources.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs), high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs), or packet voice data module (PVDM) slots to provide DSP resources.

Examples

The following shows sample output from several forms of the **show dsp-group** command. The fields are self explanatory.

```
Router# show dsp-group all

DSP groups on slot 0:
dsp 1:
  State: UP, firmware: 28.0.103
  Max signal/voice channel: 32/32
  Max credits: 480, Voice credits: 0, Video credits: 480
  num_of_sig_chnls_allocated: 32
  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VIDEO_POOL, complexity: FLEX
    Video Credits Max: 480, Share: 0, Reserved (rounded-up): 480
    Video Group: VIDEO_CONF, rsc id: 2, mode: VCONF_HETE
      Session: 0, maximum participants: 4
        Video Transcoding channels reserved credits: 480
        Video Transcoding channels allocated: 1
          Encoder: inactive, credit reserved: 480
  Slot: 0
  Device idx: 0
  PVDM Slot: 0
```

```
  Dsp Type: SP2600

dsp 2:
  State: UP, firmware: 28.0.103
  Max signal/voice channel: 32/32
  Max credits: 480, Voice credits: 0, Video credits: 480
  num_of_sig_chnls_allocated: 32
  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VIDEO_POOL, complexity: FLEX
    Video Credits Max: 480, Share: 0, Reserved (rounded-up): 480
    Video Group: VIDEO_CONF, rsc id: 2, mode: VCONF_HETE
      Session: 0, maximum participants: 4
        Video Transcoding channels reserved credits: 480
        Video Transcoding channels allocated: 3
          Decoder: inactive, credits reserved: 160
          Decoder: inactive, credits reserved: 160
          Decoder: inactive, credits reserved: 160
  Slot: 0
  Device idx: 0
  PVDM Slot: 0
  Dsp Type: SP2600

DSP groups on slot 1:
 This command is not applicable to slot 1

DSP groups on slot 2:
 This command is not applicable to slot 2

DSP groups on slot 3:
 This command is not applicable to slot 3
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
voice service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources. This command is required to enable video services.
voice-card	Enters voice-card configuration mode.

show echo-cancel

To display the echo-cancellation information of T1/E1 multiflex voice/WAN interface cards, use the **show echo-cancel** command in privileged EXEC mode.

show echo-cancel hardware status *slot-number*

Syntax Description

hardware	Displays information about the hardware accelerated EC device.
status	Displays the allocation status.
slot-number	The slot number of the interface cards.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

Hardware echo cancellation is restricted to the same baseboard voice/WAN interface card (VWIC) on which the daughter card (EC-MFT-32 and EC-MFT-64) is installed and cannot be shared by other T1/E1 controllers.

Examples

The following is sample output from the **show echo-cancel hardware status** command:

```
Router# show echo-cancel hardware status

ECAN CH   Assigned   DSP ID   VOICEPORT   EC   NLP   COV  LAW
============================================================
   0          yes       8       1/0/0      on   off   on   u-Law
   1          no        -          -       off  on    on   u-Law
   2          no        -          -       off  on    on   u-Law
   3          no        -          -       off  on    on   u-Law
   4          no        -          -       off  on    on   u-Law
   5          no        -          -       off  on    on   u-Law
```

Table 100 describes the significant fields shown in the display.

Table 100 show echo-cancel Field Descriptions

Field	Description
ECAN CH	Total channels in the slot.
Assigned	Status of the assigned channels.
DSP ID	Digital Signaling Processor (DSP) identification number for the assigned channels.
VOICEPORT	Voice port of the channels.

Table 100 show echo-cancel Field Descriptions (continued)

Field	Description
EC	Echo Cancellation status of the assigned channels.
NLP	Status of the Non-Linear Processor (NLP).
COV	Echo cancellation Coverage status of the assigned channels.

show event-manager consumers

To display event-manager statistics for debugging purposes, use the **show event-manager consumers** command in privileged EXEC mode.

show event-manager consumers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows one call (two call legs) going through the gateway:

```
Router# show event-manager consumers

Hash table indexed by AAA_UNIQUE_ID
Uid        Consumer_id  Consumer_hdl  evt_type
00000015   0002         65B35570      START
00000015   0002         65B35570      STOP
00000016   0002         65B34ECC      START
00000016   0002         65B34ECC      STOP
```

Table 1 lists and describes the significant output fields.

Field	Description
Uid	User ID.
Consumer_id	ID of the consumer client process.
Consumer_hdl	Handler of the consumer client process.
evt_type	Event type.

Related Commands

Command	Description
show voice statistics csr interval accounting	Displays all accounting CSRs specified by interval number.
show voice statistics csr interval aggregation	Displays signaling CSRs specified by interval number.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.

Command	Description
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.

show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link connection identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

show frame-relay vofr [*interface* [*dlci* [*cid*]]]

Syntax Description

interface	(Optional) Specific interface type and number for which you wish to display FRF.11 subchannel information.
dlci	(Optional) Specific data link connection identifier for which you wish to display FRF.11 subchannel information.
cid	(Optional) Specific subchannel for which you wish to display information.

Defaults

If this command is entered without a specified interface, FRF.11 subchannel information is displayed for all VoFR interfaces and DLCIs configured on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Examples

The following is sample output from this command when an interface is not specified:

```
Router# show frame-relay vofr

interface         vofr-type   dlci   cid   cid-type
Serial0/0.1       VoFR        16     4     data
Serial0/0.1       VoFR        16     5     call-control
Serial0/0.1       VoFR        16     10    voice
Serial0/1.1       VoFR cisco  17     4     data
```

The following is sample output from this command when an interface is specified:

```
Router# show frame-relay vofr serial0

interface         vofr-type   dlci   cid   cid-type
Serial0           VoFR        16     4     data
Serial0           VoFR        16     5     call-control
Serial0           VoFR        16     10    voice
```

The following is sample output from this command when an interface and a DLCI are specified:

```
Router# show frame-relay vofr serial0 16

VoFR Configuration for interface Serial0

dlci vofr-type  cid cid-type          input-pkts    output-pkts   dropped-pkts
16   VoFR       4   data              0             0             0
16   VoFR       5   call-control      85982         86099         0
16   VoFR       10  voice             2172293       6370815       0
```

The following is sample output from this command when an interface, a DLCI, and a CID are specified:

```
Router# show frame-relay vofr serial0 16 10

VoFR Configuration for interface Serial0 dlci 16

  vofr-type  VoFR     cid 10      cid-type voice
  input-pkts 2172293   output-pkts 6370815   dropped-pkts 0
```

Table 101 describes significant fields shown in this output.

Table 101 show frame-relay vofr Field Descriptions

Field	Description
interface	Number of the interface that has been selected for observation of FRF.11 subchannels.
vofr-type	Type of VoFR DLCI being observed.
cid	Portion of the specified DLCI that is carrying the designated traffic type. A DLCI can be subdivided into 255 subchannels.
cid-type	Type of traffic carried on this subchannel.
input-pkts	Number of packets received by this subchannel.
output-pkts	Number of packets sent on this subchannel.
dropped-pkts	Total number of packets discarded by this subchannel.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show voice-port	Displays configuration information about a specific voice port.

show gatekeeper calls

To display the status of each ongoing call of which a gatekeeper is aware, use the **show gatekeeper calls** command in privileged EXEC mode.

show gatekeeper calls [**history**]

Syntax Description

history	(Optional) Displays call history information along with internal error codes at the gatekeeper. The number of disconnected calls displayed in response to this command is the **number** specified in the **call-history max-size number** command. Use of this **max-size** number helps to reduce CPU usage in the storage and reporting of this information.

Command Default

The default expression of this command displays information for all active calls detected on the gatekeeper.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.0(5)T	The output for this command was changed.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.4(4)T	The **history** keyword was added to display historical information on disconnected calls.

Usage Guidelines

Use this command to show all active calls currently being handled by a particular Multimedia Conference Manager (MCM) gatekeeper. If you force a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system does not display information about those calls.

Using the **history** keyword displays the number of disconnected calls specified in the **call-history max-size number** command. Use of this **max-size** number helps to reduce CPU usage in the storage and reporting of this information.

Examples

The following is sample output showing active calls:

```
Router# show gatekeeper calls

Total number of active calls = 1.
                        GATEKEEPER CALL INFO
                        ====================
LocalCallID                          Age(secs)   BW
12-3339                              94          768(Kbps)
 Endpt(s):Alias        E.164Addr     CallSignalAddr  Port  RASSignalAddr   Port
   src EP:epA                        10.0.0.0        1720  10.0.0.0        1700
   dst EP:epB@zoneB.com
   src PX:pxA                        10.0.0.0        1720  10.0.0.00       24999
   dst PX:pxB                        255.255.255.0   1720  255.255.255.0   24999
```

Table 102 describes the significant fields shown in the display.

Table 102 show gatekeeper calls Field Descriptions

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	Age of the call, in seconds.
BW(Kbps)	Bandwidth in use, in kilobytes per second.
Endpt	Role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy) and the call signaling and Registration, Admission, and Status (RAS) protocol address.
Alias	H.323-Identification (ID) or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call-signaling IP address of the endpoint.
Port	Call-signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

Related Commands

Command	Description
clear h323 gatekeeper call	Forces the disconnection of a specific call or of all calls active on a particular gatekeeper.
call history max	Specifies the number of records to be kept in the history table.

show gatekeeper circuits

To display the circuit information on a gatekeeper, use the **show gatekeeper circuits** command in privileged EXEC mode.

show gatekeeper circuits [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

|begin	(Optional) Displays all circuits, beginning with the line containing the *expression.*
|exclude	(Optional) Displays all circuits, excluding those containing the *expression.*
|include	(Optional) Displays all circuits, including those containing the *expression.*
expression	(Optional) Word or phrase used to determine what lines are displayed.

Defaults

Shows all circuit information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to display current configuration information about the circuits that are registered with the gatekeeper.

Examples

The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper circuits

Circuit       Endpoint   Max Calls Avail Calls Resources     Zone
-------       --------   --------- ----------- ---------     ----
CarrierA      Total Endpoints: 2
              3640-gw1   25        25          Available
              5400-gw1   23        19          Unavailable
CarrierB      Total Zones: 1
                                                           MsPacmanGK
```

Table 103 describes the fields shown in this output.

Table 103 show gatekeeper circuits Field Descriptions

Field	Description
Circuit	Name of the each circuit connected to the gatekeeper.
Endpoint	Name of each H.323 endpoint.
Max Calls	Maximum number of calls that circuit can handle.

Table 103 show gatekeeper circuits Field Descriptions (continued)

Field	Description
Avail Calls	Number of new calls that the circuit can handle at the current time.
Resources	Whether the circuit's resources have exceeded the defined threshold limits. The **endpoint resource-threshold** command defines these thresholds.
Zone	Zone that supports the endpoint. The **zone circuit-id** command assigns a zone to an endpoint.
Total Endpoints	Total number of endpoints supported by the circuit.
Total Zones	Total number of zones supported by the circuit.

Related Commands

Command	Description
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a remote zone to a carrier.

show gatekeeper cluster

To display all the configured gatekeeper clusters information, use the **show gatekeeper cluster** command in user EXEC or privileged EXEC mode.

show gatekeeper cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release1.25	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1 and implemented on the Cisco AS5850 router.

Examples

The following is sample output from the **show gatekeeper cluster** command. Field descriptions are self-explanatory.

```
Router# show gatekeeper cluster

                    CONFIGURED CLUSTERS
                    ===================
Cluster Name    Type     Local Zone   Elements  IP
------------    ----     ----------   --------  --
Cluster A       Local    AGK1         AGK2      192.168.200.254 1719
                                      AGK3      192.168.200.223 1719
Cluster B       Remote               BGK1      192.168.200.257 1719
                                      BGK2      192.168.200.258 1719
                                      BGK3      192.168.200.259 1719
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gatekeeper performance stats	Displays the performance statistics on the the gatekeeper level message.
show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper endpoint circuits

To display the information of all registered endpoints and carriers or trunk groups for a gatekeeper, use the **show gatekeeper endpoint circuits** command in privileged EXEC mode.

show gatekeeper endpoint circuits [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Displays all circuits, beginning with the line that contains *expression.*
| exclude	(Optional) Displays all circuits, excluding those that contain *expression.*
| include	(Optional) Displays all circuits, including those that contain *expression.*
expression	(Optional) Word or phrase used to determine what lines are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.2(11)T	The display format was modified to show the E.164 ID, carrier and trunk group data, and total number of active calls.

Usage Guidelines

Use this command to display current configuration information about the endpoints and carriers registered with the gatekeeper. Note that you must type the pipe (|) before any of the optional keywords.

Examples

The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper endpoint circuits

                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type     Flags
--------------- ----- --------------- ----- ---------         ----     -----
172.18.195.120  1720  172.18.195.120  51059 LavenderGK        VOIP-GW
    E164-ID: 4081234
    H323-ID: 3640-gw1
    Carrier: CarrierA, Max Calls: 25, Available: 25
172.18.197.143  1720  172.18.197.143  57071 LavenderGK        VOIP-GW
    H323-ID: 5400-gw1
    Carrier: CarrierB, Max Calls: 23, Available: 19
    Carrier: CarrierA, Max Calls: 25, Available: 25
Total number of active registrations = 2
```

Table 104 describes the fields shown in this output.

Table 104 show gatekeeper endpoint circuits Fields

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.
Type	Endpoint type (for example, terminal, gateway, or MCU).
Flags	S—Endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
E164-ID	E.164 ID of the endpoint.
H323-ID	H.323 ID of the endpoint.
Carrier	Carrier associated with the endpoint.
Max Calls	Maximum number of calls the circuit can handle.
Available	Number of new calls the circuit can handle currently.

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a circuit to a remote zone.

show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in privileged EXEC mode.

show gatekeeper endpoints [**alternates**]

Syntax Description

alternates	(Optional) Displays information about alternate endpoints. All information normally included with this command is also displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM	The **alternates** keyword was added.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. The registration and call capacity values were added to the output display.
12.3(1)	This command was modified to reflect concurrent calls for the endpoints.

Examples

The following is sample output from this command:

```
Router# show gatekeeper endpoints

CallsignalAddr   Port  RASSignalAddr   Port   Zone Name    Type     F
---------------  ----  -------------   -----  ----------   -----    --
172.21.127.8     1720  172.21.127.8    24999  sj-gk        MCU
           H323-ID:joe@cisco.com
           Voice Capacity Max.=23  Avail.=23
           Total number of active registrations = 1
172.21.13.88     1720  172.21.13.88    1719   sj-gk        VOIP-GW   O    H323-ID:la-gw
```

Table 105 describes significant fields shown in this output.

Table 105 show gatekeeper endpoints Field Descriptions

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper identification [ID]) to which this endpoint is registered.
Type	Endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
F	S—Endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
Voice Capacity Max.	Maximum number of channels available on the endpoint.
Avail.	Current number of channels available on the endpoint.
Total number of active registrations	Total number of endpoints registered with the gatekeeper.

In the following example, the **show gatekeeper endpoints** output has been modified to reflect concurrent calls for the endpoint. If an endpoint is not reporting capacity and the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." and "Avail." will not be shown. "Current.= 2" indicates that the current active calls for the endpoint are 2.

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----  -------------   ----  ---------         ----    -----
172.18.200.27   1720  172.18.200.27   49918 GK-1              VOIP-GW
    H323-ID:GW1
    Voice Capacity Max.=  Avail.=  Current.= 2
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." and "Avail." will show reported call capacity of the endpoint as follows:

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  Flags
--------------  ----  -------------  ----  ---------          ----  -----
172.18.200.29   1720  172.18.200.29  53152 GK-2               VOIP-GW
    H323-ID:GW2
    Voice Capacity Max.= 23 Avail.= 22 Current.= 1
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." will show the maximum calls configured and "Avail." will show the available calls of the endpoint. In this example, "Voice Capacity Max.= 10" is showing that the maximum calls configured for the endpoint are 10. "Avail.= 2" shows that currently available calls for the endpoint are 2. "Current.= 8" shows that current active calls for the endpoint are 8.

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type     Flags
--------------  ----  -------------   ----  ---------         ----     -----
172.18.200.27   1720  172.18.200.27   49918 GK-1              VOIP-GW
    H323-ID:GW1
    Voice Capacity Max.= 10  Avail.= 2  Current.= 8
```

Table 106 describes significant fields in the output examples.

Table 106 show gatekeeper endpoints Field Descriptions

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) to which this endpoint is registered.
Type	The endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
Flags	S—Endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.

Related Commands

Command	Description
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
show gatekeeper endpoint circuits	Displays endpoint and carrier or trunk group call capacities.
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** command in privileged EXEC mode.

show gatekeeper gw-type-prefix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command for a gatekeeper that controls two local zones, sj-gk and la-gk:

```
Router# show gatekeeper gw-type-prefix

GATEWAY TYPE PREFIX TABLE
=========================
Prefix:12#*     (Default gateway-technology)
  Zone sj-gk master gateway list:
    10.0.0.0:1720 sj-gw1
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
  Zone sj-gk prefix 408....... priority gateway list(s):
   Priority 10:
    10.0.0.0:1720 sj-gw1
   Priority 5:
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
Prefix:7#*     (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    10.0.0.0:1720
    10.0.0.0:1720
  Zone la-gk master gateway list:
    10.0.0.0:1720 la-gw1
    10.0.0.0:1720 la-gw2
```

Table 107 describes significant fields shown in this output.

Table 107 show gatekeeper gw-type-prefix Field Descriptions

Field	Description
Prefix	Technology prefix defined with the **gw-type-prefix** command.
Zone sj-gk master gateway list	List of all the gateways registered to zone sj-gk with the technology prefix under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408..... priority gateway list(s)	List of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed following "Priority 10" are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, gateway sj-gw1 is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	Indication that the displayed gateway has sent a "low-in-resources" notification.
(Hopoff zone la-gk)	Any call that specifies this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls that specify technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	List of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways that register with 12# are the default type to be used for the call.
Statically-configured gateways	List of all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that, when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they are considered to be of type 7#.

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper performance statistics

To display performance statistics on the gatekeeper level message, use the **show gatekeeper performance stats** command in user EXEC or privileged EXEC mode.

show gatekeeper performance statistics [**zone** [**name** *zone-name*]] [**cumulative**]

Syntax Description

zone	(Optional) Displays zone statistics of the gatekeeper.
name *zone-name*	(Optional) Specifies the zone name or gatekeeper name.
cumulative	(Optional) Displays the total statistics collected by the gatekeeper since the last reload.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T1	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was modified. The **zone**, **name**, and **cumulative** keywords were added and the *zone-name* argument was added.
12.4(5)	This command was modified. Command output was enhanced to include counters for: • Automatic rejections (ARJs) sent due to an ARQ access-list denial. • Location rejections (LRJs) sent due to an LRQ access-list denial.

Usage Guidelines

Use this command to display the statistics on calls, registration, calls routed to other gatekeepers, and calls used via zone processing.

When the **cumulative** keyword is used along with **zone name** keywords displays the total statistics for the specified zone, from the starting time of the gatekeeper. These values are not reset when the **clear h323 gatekeeper stats** command is used.

This command displays statistical data related to the router. You can identify the number of call initiation events using the following messages:

- Automatic repeat request (ARQ)
- Admission confirmation (ACF)
- Admission rejection (ARJ)

You can identify endpoint contact events that have been requested and either confirmed or rejected on the router using the following:

- Location request (LRQ)
- Location confirm (LCF)
- Location reject (LRJ)

The counts associated with overload and the number of endpoints sent to alternate gatekeepers that are associated with overload conditions are also displayed. Only when the router experiences an overload condition do these counters reveal a value other than zero. The real endpoint count simply displays the number of endpoints registered on this router platform. The time stamp displays the start time when the counters started capturing the data. When you want to request a new start period, enter the **clear h323 gatekeeper stats** command. The counters are reset and the time stamp is updated with the new time.

You can identify remote gatekeeper contacts that have been requested and either confirmed or rejected on the router using the following messages:

- Location confirm (LCF)
- Location rejection (LRJ)
- Location request (LRQ)

You can identify zone-level or gatekeeper-level registration statistics using the following messages:

- Registration confirmation (RCF)
- Registration rejection (RRJ)
- Registration request (RRQ)

You can identify zone-level or gatekeeper-level unregistration statistics using the following messages:

- Unregistration confirmation (UCF)
- Unregistration rejection (URJ)
- Unregistration request (URQ)

Examples

The following is the example of basic output from the **show gatekeeper performance stats** command. The basic output specifies that the counters are reset using the **clear h323 gatekeeper stats** command and the output displays the statistcs from the last reset.

```
Router# show gatekeeper performance stats

-----Gatekeeper Performance Statistics-----

Performance statistics captured since: 20:09:00 UTC Thu Sep 15 2005


Gatekeeper level Admission Statistics:
        ARQs received: 1
        ARQs received from originating endpoints: 0
        ACFs sent: 1
        ACFs sent to the originating endpoint: 0
        ARJs sent: 0
        ARJs sent to the originating endpoint: 0
        ARJs sent due to overload: 0
        ARJs sent due to ARQ access-list denial: 0
        Number of concurrent calls: 0
        Number of concurrent originating calls: 0
```

```
Gatekeeper level Location Statistics:
        LRQs received: 3
        LRQs sent: 0
        LCFs received: 0
        LCFs sent: 1
        LRJs received: 0
        LRJs sent: 2
        LRJs sent due to overload: 0
        LRJs sent due to LRQ access-list denial: 2

Gatekeeper level Registration Statistics:
        RRJ due to overload: 0
        Total Registered  Endpoints: 2

Gatekeeper level Disengage Statistics:
        DRQs received: 1
        DRQs sent: 0
        DCFs received: 0
        DCFs sent: 1
        DRJs received: 0
        DRJs sent: 0

Gatekeeper viazone message counters:
        inARQ: 0
        infwdARQ: 0
        inerrARQ: 0
        inLRQ: 0
        infwdLRQ: 0
        inerrLRQ: 0
        outLRQ: 0
        outfwdLRQ: 0
        outerrLRQ: 0
        outARQ: 0
        outfwdARQ: 0
        outerrARQ: 0

Load balancing events: 0
```

The following is the example of cumulative output from the **show gatekeeper performance stats** command. The cumulative output specifies that the counters are not reset and the output displays the total statistcs from the starting time of the gatekeeper.

```
Router# show gatekeeper performance stats zone name voip3-2600-2

Performance statistics for zone voip3-2600-2

-----Zone Level Performance Statistics-----

Performance statistics captured since: 00:17:00 UTC Mon Mar 1 1993

Zone level Admission Statistics:
        ARQs received: 1
        ARQs received from originating endpoints: 0
        ACFs sent: 1
        ACFs sent to the originating endpoint: 0
        ARJs sent: 0
        ARJs sent to the originating endpoint: 0
        Number of concurrent total calls: 0
        Number of concurrent originating calls: 0
```

```
Zone level Location Statistics:
        LRQs received: 1
        LRQs sent: 0
        LCFs received: 0
        LCFs sent: 1
        LRJs received: 0
        LRJs sent: 0

Zone level Registration Statistics:
        Full RRQs received: 1
        Light RRQs received: 574
        RCFs sent: 576
        RRJs sent: 0
        Total Registered Endpoints: 1

Zone level UnRegistration Statistics:
        URQs received: 0
        URQs sent: 0
        UCFs received: 0
        UCFs sent: 0
        URJs received: 0
        URJs sent: 0
        URQs sent due to timeout: 0

Zone level Disengage Statistics:
        DRQs received: 1
        DRQs sent: 0
        DCFs received: 0
        DCFs sent: 1
        DRJs received: 0
        DRJs sent: 0
```

Table 108 shows significant fields shown in the displays. Most of the fields are self-explanatory and are not listed the table.

Table 108 show gatekeeper performance statistics Field Descriptions

Field	Description
Full RRQs received	A full registration request (RRQ) contains all registration information that is used for successful registration.
Light RRQs received	A light RRQ contains abbreviated registration information that is used to maintain an existing registration.

Related Commands

Command	Description
clear h323 gatekeeper stats	Clears statistics about gatekeeper performance.

show gatekeeper servers

To display a list of currently registered and statically configured triggers on a gatekeeper router, use the **show gatekeeper servers** command in EXEC mode.

show gatekeeper servers [*gkid*]

Syntax Description

gkid	(Optional) Local gatekeeper name to which this trigger applies.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200, and Cisco MC3810.
12.2(2)XB	The output of this command was modified to show additional server statistics, including the following: gatekeeper server timeout value; Gatekeeper Transaction Message Protocol (GKTMP) version installed; number of Registration Request (RRQ), Registration Response (RRQ), Response Confirmation (RCF), and Response Reject (RRJ) messages received; timeouts encountered; average response time; and if the server is usable.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco 3700 series.
12.2(15)T12	The command was modified to show additional server statistics.
12.3(8)T	The command was modified to show additional server statistics.
12.3(9)	The command was modified to show additional server statistics.

Usage Guidelines

Use this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command-line interface) on this gatekeeper. If the gatekeeper ID is specified, only triggers applied to the specified gatekeeper zone appear. If the gatekeeper ID is not specified, server triggers for all local zones on this gatekeeper appear.

Examples

The following is sample output from this command:

```
Router# show gatekeeper servers

            GATEKEEPER SERVERS STATUS
            =========================

Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 4.1
```

```
Gatekeeper-ID: Gatekeeper1
------------------------
RRQ Priority: 5
Server-ID: Server43
Server IP address: 209.165.200.254:40118
Server type: dynamically registered
Connection Status: active
Trigger Information:
Trigger unconditionally
Server Statistics:
REQUEST RRQ Sent=0
RESPONSE RRQ Received = 0
RESPONSE RCF Received = 0
RESPONSE RRJ Received = 0
Average response time(ms)=0
Server Usable=TRUE

Timeout Statistics:

Server-ID: Server43
Server IP address: 209.165.200.254:40118
Server type: dynamically registered
Connection Status: active
Timeout Encountered=0
```

Table 109 describes significant fields shown in this output.

Table 109 show gatekeeper servers Field Descriptions

Field	Description
GateKeeper GKTMP version	Version of Gatekeeper Transaction Message Protocol installed.
RRQ Priority	Registration priority.
Server-ID	Server ID name.
Server IP address	Server IP address.
Server type	Type of server.
Connection Status	Whether the connection is active or inactive.
Trigger Information	Which Registration, Admission, and Status (RAS) messages the Cisco IOS gatekeeper forwards to the external application.
REQUEST RRQ	Registration requests received.
RESPONSE RRQ	Registration responses received.
RESPONSE RCF	Response confirmations received.
RESPONSE RRJ	Response reject messages received.

Related Commands

Command	Description
debug gatekeeper server	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications.
endpoint circuit-id h323id	Tracks call capacity information on the gatekeeper.
server registration-port	Configures a listening port on the gatekeeper for server registration.
server trigger arq	Configures static triggers on the gatekeeper.

show gatekeeper status

To display overall gatekeeper status, including authorization and authentication status and zone status, use the **show gatekeeper status** command in EXEC mode.

show gatekeeper status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	This command was modified to show information about load balancing and vendor-specific attributes.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB	This command was modified to show information about server flow control.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples

The following is sample output from this command:

```
Router# show gatekeeper status

Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        snet-3660-3
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:              unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

Table 110 describes significant fields shown in this output.

Table 110 Show Gatekeeper Status Field Descriptions

Field	Description
Gatekeeper State	Gatekeeper state has the following values: • UP is operational. • DOWN is administratively shut down. • INACTIVE is administratively enabled; that is, the **no shutdown** command has been issued, but no local zones have been configured. • HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.
Load Balancing	Whether load balancing is enabled.
Flow Control	Whether server flow control is enabled.
Zone Name	Zone name to which the gatekeeper belongs.
Accounting	Whether authorization and accounting features are enabled.
Endpoint Throttling	Whether endpoint throttling is enabled.
Security	Whether security features are enabled.
Bandwidth	Maximum remote bandwidth, current remote bandwidth, and current remote bandwidth with alternate gatekeepers.

Related Commands

Command	Description
show gatekeeper servers	Displays statistics about the gatekeeper.

show gatekeeper status cluster

To display information about each element of a local cluster, such as the amount of memory used, the number of active calls, and the number of endpoints registered on the element, use the **show gatekeeper status cluster** command in privileged EXEC mode.

show gatekeeper status cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)XM1	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Examples

The following command displays information about elements of a local cluster, two of whose components are RoseGK and LavenderGK:

```
Router# show gatekeeper status cluster

                    CLUSTER INFORMATION
                    ===================
                                   Active      Endpoint        Last
Hostname      %Mem    %CPU     Calls         Count    Announce
--------      ----    ----    ------      --------    --------
RoseGK          72       0         1    Local Host
LavenderGK      30       1         0             4         14s
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gatekeeper performance statistics	Displays information about the number of calls accepted and rejected, and finds the number of endpoints sent to other gatekeepers.
show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper zone cluster

To display the dynamic status of all local clusters, use the **show gatekeeper zone cluster** command in privileged EXEC mode.

show gatekeeper zone cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)XM1	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Examples

The following command displays information about the current bandwidth values and about when the last announcement message from the alternate gatekeeper was received. In the following example, PRI represents the priority value assigned to an alternate gatekeeper. This field ranges from 0 to 127, with 127 representing the lowest priority.

```
Router# show gatekeeper zone cluster

                  LOCAL CLUSTER INFORMATION,6t
                  ============================
                                       TOT BW   INT BW   REM BW   LAST       ALT GK
LOCAL GK NAME   ALT GK NAME   PRI   (kbps)   (kbps)   (kbps)   ANNOUNCE   STATUS
-------------   -----------   ---   ------   ------   ------   --------   ------
ParisGK         GenevaGK      120   0        0        0        7s         CONNECTED
NiceGK          ZurichGK      100   0        0        0        7s         CONNECTED
```

Related Commands

Command	Description
timer cluster-element announce	Defines the time interval between successive announcement messages exchanged between elements of a local cluster.
zone cluster local	Defines a local grouping of gatekeepers.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

show gatekeeper zone prefix

To display the zone prefix table, use the **show gatekeeper zone prefix** command in privileged EXEC mode.

show gatekeeper zone prefix [**all**]

Syntax Description

all	(Optional) Displays the dynamic zone prefixes registered by each gateway.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.2(15)T	The **all** keyword was added.

Usage Guidelines

If the **all** keyword is not specified, the **show gatekeeper zone prefix** command displays the static zone prefixes only. Use the **include** filter with the **all** keyword to display the prefixes associated with a particular gateway. For example, the **show gatekeeper zone prefix all | include GW1** command displays the dynamic prefixes associated with gateway GW1.

Examples

The following command displays the zone prefix table for the gatekeeper:

```
Router# show gatekeeper zone prefix

      ZONE PREFIX TABLE
      =================
GK-NAME               E164-PREFIX
-------               -----------
gk2                   408*
gk2                   5551001*
gk2                   5551002*
gk2                   5553020*
gk2                   5553020*
gk1                   555....
gk2                   719*
gk2                   919*
```

The following command displays the zone prefix table, including the dynamic zone prefixes, for the gatekeeper:

```
Router# show gatekeeper zone prefix all

                    ZONE PREFIX TABLE
      ================================================
GK-NAME               E164-PREFIX       Dynamic GW-priority
-------               -----------       -------------------
gk2                   408*
gk2                   5551001*            GW1 /5
gk2                   5551002*            GW1 /5 GW2 /10
gk2                   5553020*            GW1 /8
gk2                   5553020*
gk1                   555....
gk2                   719*
gk2                   919*                GW2 /5
```

Table 111 describes significant fields shown in this output.

Table 111 show gatekeeper zone prefix Field Descriptions

Field	Description
GK-NAME	Gatekeeper name.
E164-PREFIX	E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number.
Dynamic GW-priority	Gateway that serves this E164 prefix. Gateway priority. A 0 value prevents the gatekeeper from using the gateway for that prefix. Value 10 places the highest priority on the gateway. The default priority value for a dynamic gateway is 5.

show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** command in privileged EXEC mode.

show gatekeeper zone status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command:

```
Router# show gatekeeper zone status

                    GATEKEEPER ZONES
                    ================
GK name      Domain Name   RAS Address     PORT  FLAGS MAX-BW   CUR-BW
                                                     (kbps)    (kbps)
-------      -----------   -----------     ----  ----- ------    ------
sj.xyz.com   xyz.com       10.0.0.0        1719  LS              0
  SUBNET ATTRIBUTES :
    All Other Subnets :(Enabled)
  PROXY USAGE CONFIGURATION :
    inbound Calls from germany.xyz.com :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to germany.xyz.com
      from terminals in local zone germany.xyz.com :use proxy
      from gateways in local zone germany.xyz.com  :do not use proxy
    Inbound Calls from all other zones :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone sj.xyz.com :do not use proxy
      from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co xyz.com         10.0.0.0        1719  RS              0
milan.xyz.co xyz.com         10.0.0.0        1719  RS              0
```

Table 112 describes significant fields shown in this output.

Table 112 show gatekeeper zone status Field Descriptions

Field	Description
GK name	Gatekeeper name (also known as the zone name), which is truncated after 12 characters in the display.
Domain Name	Domain with which the gatekeeper is associated.
RAS Address	Registration, Admission, and Status (RAS) protocol address of the gatekeeper.
FLAGS	Displays the following information: • S = static (CLI-configured, not DNS-discovered) • L = local • R = remote
MAX-BW	Maximum bandwidth for the zone, in kbps.
CUR-BW	Current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	List of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

show gateway

To display the current status of the gateway, use the **show gateway** command in privileged EXEC mode.

show gateway

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following sample output shows the report that appears when the gateway is not registered with a gatekeeper:

```
Router# show gateway

Gateway gateway1 is not registered to any gatekeeper
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled but NOT Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

This following sample output indicates that an E.164 address has been assigned to the gateway:

```
Router# show gateway

Gateway  gateway1 is registered to Gatekeeper gk1
Gateway alias list
E.164 Number 5551212
H323-ID gateway1
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is enabled with the **resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled and Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is disabled with the **no resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Disabled
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.

show h323 calls preserved

To display data about active H.323 VoIP preserved calls, use the **show h323 calls preserved** command in user EXEC or privileged EXEC mode.

show h323 calls preserved

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **show h323 calls preserved** command displays data per preserved call. Only active calls are displayed; preserved call history is not.

If translation rules are configured, the value displayed in the "Calling Number" field may have been translated by a gateway. Gateways handle called number values as the numbers to which calls are routed.

The "CallID" field displays the shorter form of the 16-octet, globally-unique connection ID that is allocated for each call leg. The show call active voice brief command also displays a shorter form of the CallID value (part of the third octet and the fourth octet). The longer form of the CallID value is output by the **show call active voice** command.

The CallID value can be used to refer to a call leg associated with the CallID when issuing other voice commands on the gateway, such as the **show voice call status** command and the **clear call voice** command.

An output value of -1 displayed in the "H225 FD" or "H245 FD" field denotes that the call was preserved due to an error detected on the H.225.0 connection. The actual H.225.0 socket file descriptor used for this call can be found from the syslog message that was output when this call was preserved.

To obtain more information about a call, you can also use the **show call active voice** command. Calls can be cleared with the **clear call voice causecode** command.

Examples

The following is sample output from the **show h323 calls preserved** command where one active call is preserved:

```
Router# show h323 calls preserved

CallID = 11EC , Calling Number = , Called Number = 3210000 ,
RemoteSignallingIPAddress=9.13.0.26 , RemoteSignallingPort=49760 ,
RemoteMediaIPAddress=9.13.0.11 , RemoteMediaPort=17910 , Preserved Duration = 262 , Total
Duration = 562 , H225 FD = -1 , H245 FD = -1
```

Table 111 provides an alphabetical listing of the fields displayed in the output of the **show h323 calls preserved** command and a description of each field.

Table 111 show h323 calls preserved Field Descriptions

Field	Description
Called Number	The phone number entered by the caller.
CallID	The shortened name for connection ID displayed in the **show call active voice brief** command.
H225 FD	The file descriptor number of the H.225.0 TCP socket.
H245 FD	The file descriptor number of the H.245 TCP socket.
Preserved Duration	The time in seconds that the call has been preserved.
RemoteMediaIPAddress	The remote media IP address.
RemoteMediaPort	The remote media IP address.
RemoteSignallingIPAddress	The remote signaling IP address.
RemoteSignallingPort	The remote signaling port.
Total Duration	The time in seconds of the phone call.

Related Commands

Command	Description
call preserve	Enables the preservation of H.323 VoIP calls.
clear call voice	Clears one or more voice calls detected as inactive because there is no RTP or RTCP activity.
show call active voice	Displays call information for voice calls in progress.
show voice call	Displays the call status for voice ports on the Cisco router.

show h323 gateway

To display statistics for H.323 gateway messages that have been sent and received and to display the reasons for which H.323 calls have been disconnected, use the **show h323 gateway** command in privileged EXEC mode.

show h323 gateway [**cause-code stats** | **h225** | **ras**]

Syntax Description

cause-code stats	(Optional) Output displays the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway.
h225	(Optional) Output lists cumulative counts of the number of H.225 messages that have been sent and received since the counters were last cleared.
ras	(Optional) Output lists the counters for Registration, Admission, and Status (RAS) messages that have been sent to and received from the gatekeeper since the counters were last cleared.

Command Default

To display statistics for all the options, use this command without any of the optional keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced on Cisco H.323 platforms except for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

In the following example from a Cisco 3640 router, this command is used without keywords to display the statistics for all the options. See Table 112, Table 113, and Table 114 for descriptions of the fields.

```
Router# show h323 gateway

H.323 STATISTICS AT 01:45:55

H.225 REQUESTS      SENT    RECEIVED    FAILED
Setup               0       5477        0
Setup confirm       5424    0           0
Alert               2734    0           0
Progress            2701    0           0
Call proceeding     5477    0           0
Notify              0       0           0
Info                0       0           0
User Info           0       0           0
Facility            2732    0           0
Release             5198    5313        241
Reject              0       0           0
Passthrough         0       0           0

H225 establish timeout 0
RAS failed            0
```

```
H245 failed           0

RAS MESSAGE      REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
GK Discovery     grq 0            gcf 0            grj 0
Registration     rrq 130          rcf 130          rrj 0
Admission        arq 5477         acf 5477         arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 5439         dcf 5439         drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0

RAS MESSAGE      REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
GK Discovery     grq 0            gcf 0            grj 0
Registration     rrq 0            rcf 0            rrj 0
Admission        arq 0            acf 0            arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 0            dcf 0            drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0

DISC CAUSE CODE           FROM OTHER PEER    FROM H323 PEER
16 normal call clearing   66                 5325
31 normal, unspecified    1                  0
34 no circuit             31                 0
41 temporary failure      3                  0
44 no requested circuit   13                 0
```

In the following example from a Cisco 3640 router, this command is used with the **cause-code stats** keyword to display the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway. Only the nonzero cause-code counts are displayed.

```
Router# show h323 gateway cause-code stats

CAUSE CODE STATISTICS AT 01:40:25

DISC CAUSE CODE           FROM OTHER PEER      FROM H323 PEER
16 normal call clearing   66                   4976
31 normal, unspecified    1                    0
34 no circuit             31                   0
41 temporary failure      3                    0
44 no requested circuit   13                   0
```

Table 112 describes significant fields shown in this output

Table 112 show h323 gateway cause-code stats Field Descriptions

Field	Description
Column Headings:	
DISC CAUSE CODE	Decimal value of the cause code, followed by the textual description.
FROM OTHER PEER	Number of disconnects that have been received from the opposite call leg for each cause code (for example, from a PRI T1 POTS peer or a Foreign exchange station [FXS] POTS peer).
FROM H323 PEER	Number of disconnects that have been received from the far-end gateway for each cause code.
Fields listed under the headings are self-explanatory.	

In the following example from a Cisco 3640 router, this command is used with the **h225** keyword to display the cumulative counts of the number of H.225 messages that were sent and received since the counters were last cleared.

Each row shows the sent, received, and failed counts for one type of H.225 request. If the counters have not been cleared, total counts are shown for the router since it was last reloaded.

```
Router# show h323 gateway h225

H.225 STATISTICS AT 00:44:57

H.225 REQUESTS          SENT    RECEIVED    FAILED
Setup                   1654    0           0
Setup confirm           0       1654        0
Alert                   0       828         0
Progress                0       826         0
Call proceeding         0       1654        0
Notify                  0       0           0
Info                    0       0           0
User Info               0       0           0
Facility                0       828         0
Release                 1613    9           1
Reject                  0       0           0
Passthrough             0       0           0

H225 establish timeout  0
RAS failed              1
H245 failed             0
```

Table 113 describes significant fields shown in this output.

Table 113 show h323 gateway h225 Field Descriptions

Field	Description
Column Headings:	
H.225 REQUESTS	Types of H.225 messages.
SENT	Number of H.225 messages sent by the gateway.
RECEIVED	Number of H.225 messages received from a remote gateway or endpoint.
FAILED	Number of H.225 messages that could not be sent. A failure could occur if, for example, the H.323 subsystem tried to send an H.225 release request but the TCP socket had already been closed.
Fields:	
Setup	Number of setup messages that were sent, that were received, or that could not be sent. This message is sent by a calling H.323 entity to indicate its desire to set up a connection to the called entity.
Setup confirm	Number of setup confirm messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to acknowledge receipt of a setup message.
Alert	Number of alert messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that called user alerting has been initiated. (In everyday terms, the “phone is ringing.”)

Table 113 show h323 gateway h225 Field Descriptions (continued)

Field	Description
Progress	Number of progress messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to indicate the progress of a call.
Call proceeding	Number of call proceeding messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that requested call establishment has been initiated and that no more call establishment information is accepted.
Notify	Number of notify messages that were sent, that were received, or that could not be sent.
Info	Number of information messages that were sent, that were received, or that could not be sent.
User Info	Number of user information messages that were sent, that were received, or that could not be sent. This message may be used to provide additional information for call establishment (for example, overlap signaling), to provide miscellaneous call-related information, or to deliver proprietary features.
Facility	Number of facility messages that were sent, that were received, or that could not be sent. This message is used to provide information on where a call should be directed or for an endpoint to indicate that the incoming call must go through a gatekeeper.
Release	Number of release complete messages that were sent, that were received, or that could not be sent. This message is sent by a gateway to indicate the release of the call if the reliable call signaling channel is open.
Reject	Number of reject messages that were sent, that were received, or that could not be sent.
Passthrough	Number of pass-through messages that were sent, that were received, or that could not be sent.
H225 establish timeout	Number of times the H.323 subsystem was unable to establish an H.225 connection to a remote gateway for a call.
RAS failed	Number of times an Admission Reject (ARJ) or Disengage Reject (DRJ) message is received from the gatekeeper. This counter should equal the arj + drj received counters shown in the **show h323 gateway ras** command output.
H245 failed	Number of times the H.323 subsystem was unable to create an H.245 tunnel for a call or was unable to send an H.245 message.

In the following example from a Cisco 3640 router, this command is used with the **ras** keyword to display the counters for Registration, Admission, and Status (RAS) messages that were sent to the gatekeeper and received from the gatekeeper. With the exception of the Resource Avail and Req In Progress messages, each RAS message has three variations: a request message, a confirm message, and a reject message. For example, for the Admission message type, there is an Admission Request (arq) message, an Admission Confirm (acf) message, and an Admission Reject (arj) message. The gateway sends the arq message, and the gatekeeper responds with either an acf or an arj message, depending on whether the gatekeeper confirms or rejects the admission request.

Each of the two tables that follow lists the same message types, with each row showing a different message type. The first table shows the requests sent, the confirms received, and the rejects received. The second table shows the requests received, the confirms sent, and the rejects sent. Some rows in the second table would apply only to the gatekeeper (for example, a gateway would never receive a Registration Request (rrq) message, send a Registration Confirmation (rcf) message, or send a Registration Rejection (rrj) message).

```
Router# show h323 gateway ras

RAS STATISTIC AT 01:10:01

RAS MESSAGE      REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
GK Discovery     grq 3            gcf 1            grj 0
Registration     rrq 73           rcf 73           rrj 0
Admission        arq 3216         acf 3215         arj 1
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 3174         dcf 3174         drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0

RAS MESSAGE      REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
GK Discovery     grq 0            gcf 0            grj 0
Registration     rrq 0            rcf 0            rrj 0
Admission        arq 0            acf 0            arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 0            dcf 0            drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0
```

Table 114 describes significant fields shown in this output.

Table 114 show h323 gateway ras Field Descriptions

Field	Description
Column Headings for the First Table:	
RAS MESSAGE	Type RAS message.
REQUESTS SENT	Number of RAS request messages sent by the gateway to a gatekeeper.
CONFIRMS RCVD	Number of RAS confirmation messages received from a gatekeeper.
REJECTS RCVD	Number of RAS reject messages received from a gatekeeper.
Column Headings for the Second Table:	
RAS MESSAGE	Type of RAS message.
REQUESTS RCVD	Number of RAS request messages received from a gatekeeper.
CONFIRMS SENT	Number of RAS confirmation messages sent by the gateway.
REJECTS SENT	Number of RAS reject messages sent by the gateway.
Fields:	
GK Discovery	Gatekeeper Request (GRQ) message requests that any gatekeeper receiving it respond with a Gatekeeper Confirmation (GCF) message granting it permission to register. The Gateway Reject (GRJ) message is a rejection of this request, indicating that the requesting endpoint should seek another gatekeeper.

Table 114 show h323 gateway ras Field Descriptions (continued)

Field	Description
Registration	Registration Request (RRQ) message is a request from a terminal to a gatekeeper to register. If the gatekeeper responds with a Registration Confirmation (RCF) message, the terminal uses the responding gatekeeper for future calls. If the gatekeeper responds with a Registration Reject (RRJ) message, the terminal must seek another gatekeeper with which to register.
Admission	Admission Request (ARQ) message requests that an endpoint be allowed access to the packet-based network by the gatekeeper, which either grants the request with an Admission Confirmation (ACF) message or denies it with an Admission Reject (ARJ) message.
Bandwidth	Bandwidth Request (BRQ) message requests that an endpoint be granted a changed packet-based network bandwidth allocation by the gatekeeper, which either grants the request with a Bandwidth Confirmation (BCF) message or denies it with a Bandwidth Reject (BRJ) message.
Disengage	If sent from an endpoint to a gatekeeper, the Disengage Request (DRQ) message informs the gatekeeper that an endpoint is being dropped. If sent from a gatekeeper to an endpoint, the DRQ message forces a call to be dropped; such a request is not refused. The DRQ message is not sent directly between endpoints.
Unregister	UnRegistration Request (URQ) message requests that the association between a terminal and a gatekeeper be broken. Note that the URQ request is bidirectional; that is, a gatekeeper can request a terminal to consider itself unregistered, and a terminal can inform a gatekeeper that it is revoking a previous registration.
Resource Avail	Resource Availability Indication (RAI) message is a notification from a gateway to a gatekeeper of its current call capacity for each H-series protocol and data rate for that protocol. The gatekeeper responds with a Resource Availability Confirmation (RAC) message upon receiving an RAI message to acknowledge its reception.
Req In Progress	Request In Progress (RIP) message can be used by a gateway or gatekeeper when a response to a message cannot be generated within a typical retry timeout period. The RIP message specifies the time period after which a response should have been generated.

Related Commands

Command	Description
show h323 gateway prefixes	Displays the status of the destination-pattern database and the status of the individual destination patterns.

show h323 gateway prefixes

To display the status of the destination-pattern database and the status of the individual destination patterns, use the **show h323 gateway prefixes** command in privileged EXEC mode.

show h323 gateway prefixes

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines Use the **show h323 gateway prefixes** command to display the destination patterns from the active plain old telephone service (POTS) dial peers, the current state of the destination pattern (whether they have been sent to or acknowledged by the gatekeeper), and whether advertisement of dynamic prefixes is enabled on the gateway.

Examples The following command displays the status of the gateway's destination-pattern database:

```
Router# show h323 gateway prefixes

GK Supports Additive RRQ         : True
GW Additive RRQ Support Enabled  : True
Pattern Database Status          : Active


Destination                                        Active
Pattern                          Status            Dial-Peers
============================================================
1110509*                         ADD ACKNOWLEDGED      2
1110511*                         ADD ACKNOWLEDGED      2
23*                              ADD ACKNOWLEDGED      2
```

Table 115 describes the significant fields shown in the display.

Table 115 show h323 gateway prefixes Field Descriptions

Field	Description
Pattern Database Status	Status of the gateway's destination-pattern database: active or inactive.
Status	Status of the destination pattern. The status can be one of the following values: ADD PENDING—The gateway has a prefix that is waiting to be sent to the gatekeeper. Prefixes are sent only at the lightweight registration request (RRQ) RAS message schedule, which is every 30 seconds. ADD SENT—The gateway sent the prefix to the gatekeeper and is waiting for it to be acknowledged by a registration confirm (RCF) RAS message. ADD ACKNOWLEDGED—The gateway received an RCF message indicating that the gatekeeper accepted the prefix. This is the normal status when dynamic zone prefix registration is working properly. ADD REJECTED—The gatekeeper did not accept the prefix and sent a registration reject (RRJ) RAS message. One reason for rejection could be that the gatekeeper already has this prefix registered for a different zone, either by static zone prefix configuration, or because another gateway in a different zone dynamically registered this prefix first. DELETE PENDING—The prefix has gone out of service, for example, because the dial peer shut down, and the gateway is waiting to send an unregistration request (URQ) RAS message to the gatekeeper to remove it. URQ messages are sent at the lightweight RRQ schedule, which is every 30 seconds. DELETE SENT—The gateway sent a URQ message to remove the prefix to the gatekeeper. There is no DELETE ACKNOWLEDGED status. If the prefix is subsequently brought back in service, the status goes back to ADD PENDING.

Related Commands

Command	Description
show h323 gateway	Displays statistics for H.323 gateway messages that have been sent and received and the reasons for which H.l323 calls have been disconnected.

show http client cache

To display information about the entries contained in the HTTP client cache, use the **show http client cache** command in user EXEC or privileged EXEC mode.

show http client cache [**brief**]

Syntax Description

brief	(Optional) Displays summary information about the HTTP client cache.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.
12.4(15)T	The command output was modified to display files cached with URLs of HTTP and HTTPS format in separate tables. The command output was modified to mask out values of the URL attributes when caching of query data returned from the HTTP server is enabled.
12.4(15)XY	A pound sign (#) was added next to the Age field in the command output to indicate entries marked stale manually.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command:

```
Router# show http client cache

HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 100000 K-bytes
Maximum file size allowed for caching = 10 K-bytes
Total memory used up for Cache = 18837 Bytes
Message response timeout = 10 secs
Total cached entries     = 5
Total non-cached entries = 0

                              Cached entries
                              ==============
Cached table entry 167,  number of cached entries = 2
 Request URL                              Ref   FreshTime  Age        Size
 -----------                              ---   ---------  ---        ----
 abc.com/vxml/menu.vxml                   0     20         703        319
```

```
 abc.com/vxml/opr.vxml                     0     647424     646        2772
Cached table entry 171,  number of cached entries = 1
 Request URL                               Ref   FreshTime  Age        Size
 -----------                               ---   ---------  ---        ----
 onlineshop.com/catalog/advance.vxml       0     69077      1297649    3453
Cached table entry 172,  number of cached entries = 1
 Request URL                               Ref   FreshTime  Age        Size
 -----------                               ---   ---------  ---        ----
 theater.com/vxml/menu_main.vxml           0     86400      1297661    8734
Cached table entry 176,  number of cached entries = 1
 Request URL                               Ref   FreshTime  Age        Size
 -----------                               ---   ---------  ---        ----
 popcorn.com/menu/selection.vxml           1     20         7          3559
```

In the following example, the **set http client cache stale** command was used to set all the entries in the HTTP client cache to stale. Stale entries are indicated by a pound sign (#) next to the Age field.

```
Router# show http client cache

HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 20000 K-bytes
Maximum file size allowed for caching = 1000 K-bytes
Total memory used up for Cache = 37758 Bytes
Message response timeout = 10 secs
Total cached entries = 7
Total non-cached entries = 0

           Cached entries
           ==============

entry 142, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
0     30         53233       # 486      63D8FCC4
url: http://goa/TEST1.vxml

entry 145, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     4001998    53218       # 151      0
url: http://win2003/TEST2.vxml

entry 157, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     30         28          # 185      0
url: http://goa/TEST3.vxml

entry 164, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 1183     0
url: http://goa/audio/en_welcome.au

entry 166, 2 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 4916     0
url: http://goa/audio/en_one.au
1     2231127    53229       # 4500     0
url: http://goa/audio/en_three.au

entry 169, 1 entries
```

```
Ref    FreshTime  Age            Size      context
---    ---------  ---            ----      -------
1      2231127    53229       # 7224      0
url: http://goa/audio/en_two.au
```

Table 116 describes the fields shown in this output.

Table 116 show http client cache Field Descriptions

Field	Description
Maximum memory pool allowed for HTTP Client caching	Maximum amount of memory available for the HTTP client to store cached entries in kilobytes. This value is configured by using the **http client cache memory** command.
Maximum file size allowed for caching	Maximum size of a file that can be cached, in kilobytes. If a file exceeds this limit, it cannot be cached. This value is configured by using the **http client cache memory** command.
Total memory used up for Cache	Total amount of memory that is currently being used to store cached entries in kilobytes.
Total cached entries	Total number of cached entries.
Total non-cached entries	Total number of temporary, one-time used HTTP entries that are not currently cached.
Cached table entry	Index marker of the cached table entry. Each cached table entry can contain multiple URLs that were requested and cached.
number of cached entries	Number of URL entries in the cached table entry.
Request URL	URL of the cached entry.
Ref	Whether the cached entry is still in use by the application. 0 means the entry has been freed; 1 or more means that the entry is still being used by that number of applications.
FreshTime	Lifetime of a cached entry, in seconds. When an entry is the same age or older than the refresh time, the entry expires. When a request is made to a cached entry that has expired, the HTTP client sends the server a conditional request for an update. This value is configured on the HTTP server or by using the **http client cache refresh** command on the gateway.
Age	Time for which the entry has been in the cache, in seconds. • Pound sign (#) indicates entries marked stale manually. • Asterisk (*) indicates entries that have become stale without manual intervention.
Size	Size of the cached entry, in bytes.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client cache refresh	Configures the HTTP client cache refresh time.
http client response timeout	Configures the HTTP client server response timeout.
set http client cache stale	Sets the status of all entries in the HTTP client cache to stale.
show http client connection	Displays current HTTP client connection information.

show http client connection

To display the current configuration values for HTTP client connections to HTTP servers, use the **show http client connection** command in user EXEC or privileged EXEC mode.

show http client connection

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

In this command, the values for the following commands are shown:

- **http client connection idle timeout** as "connection idle timeout"
- **http client connection persistent** as "persistent connection"
- **http client connection timeout** as "initial socket connection timeout"

Note For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command:

```
Router# show http client connection

     HTTP Client Connections:
     ========================
Persistent connection   = enabled
Initial socket connection timeout = 10 secs
Connection idle timeout = 60 secs
Total HTTP server connections = 0
```

Table 117 describes the fields shown in this output.

Table 117 show http client connection Field Descriptions

Field	Description
Persistent connection	Whether HTTP keepalive connections have been enabled by using the **http client connection persistent** command.
Initial socket connection timeout	Number of seconds for which the HTTP client waits for a server to establish a connection before giving up. This value is set by using the **http client connection timeout** command.
Connection idle timeout	Number of seconds for which the HTTP client waits before terminating an idle connection. This value is set by using the **http client connection idle timeout** command.
Total HTTP server connections	Total number of current connections to an HTTP server.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client connection idle timeout	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.
http client connection persistent	Enables HTTP persistent connections so that multiple files can be loaded using the same connection.
http client connection timeout	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before giving up.
http client response timeout	Configures the HTTP client server response.

show http client cookie

To display cookies that are stored by the HTTP client, use the **show http client cookie** command in privileged EXEC mode.

show http client cookie [**id** *call-id*]

Syntax Description

id *call-id*	(Optional) Displays cookies for the specified call only.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the *call-id* argument to display cookies for a specific call; otherwise, this command displays cookies for all calls. Cookies are stored only for the duration of a call. When a call terminates, all associated cookies are deleted. If you use the *call-id* argument and the call is not active, cookies are not displayed and an error message indicates that the call is not active.

Use the **show call active voice brief** command to display the *call-id* for an active call.

Examples

The following is sample output from the **show http client cookie** command:

```
Router# show http client cookie id 144567

HTTP Client Cookies
===================
TestCookieY==password Path=/ Domain=.cisco.com
TestCookieX==username Path=/ Domain=.cisco.com
```

The output lists the name, path, and domain of the cookie. Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug http client cookie	Displays debugging traces related to HTTP cookies.
http client cache memory	Configures the memory limits for the HTTP client cache.
http client cache refresh	Configures the refresh time for the HTTP client cache.
http client cookie	Enables the HTTP client to send and receive and cookies.
show call active voice brief	Displays a call information summary for active calls.
show http client cache	Displays current HTTP client cache information.

show http client history

To display a list of the last 20 requests made by the HTTP client to the server, use the **show http client history** command in user EXEC or privileged EXEC mode.

show http client history

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command, showing the most recent GET and POST requests from the HTTP client to the server:

```
Router# show http client history

   POST http://banks.com/servlets/account
   GET http://banks.com/GetDigit.vxml
   GET http://banks.com/form.vxml
   GET http://onlineshop.com/menu.vxml
   POST http://onlineshop.com/servlets/order
   GET http://weather.com/servlets/weather?city=SanFrancisco&state=CA
```

Output shows only requests. There are no field headings.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

show http client secure status

To display the trustpoint and cipher suites that are configured in the HTTP client, use the **show http client secure status** command in user EXEC or privileged EXEC mode.

show http client secure status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command displays the trustpoint and cipher suites configured in the HTTP client by the **http client secure-trustpoint** and **http client secure-ciphersuite** commands.

Examples

The following sample output shows that the trustpoint myca has all five cipher suites configured:

```
Router# show http client secure status

HTTP Client Secure Ciphersuite: rc4-128-md5 rc4-128-sha 3des-cbc-sha des-cbc-sha null-md5
HTTP Client Secure Trustpoint: myca
```

Table 118 describes the significant fields shown in the display.

Table 118 show http client secure status Field Descriptions

Field	Description
HTTP Client Secure Ciphersuite	Cipher suites. • 3des_cbc_sha—Triple DES (Data Encryption Standard) encryption and the SHA (Secure Hash Algorithm) integrity method. • des_cbc_sha—DES encryption and the SHA integrity method. • null_md5—NULL encryption and the MD5 (Message-Digest algorithm 5) integrity method. • rc4_128_md5—RC4 (or ARCFOUR) encryption and the MD5 integrity method. • rc4_128_sha—RC4 encryption and the SHA integrity method.
HTTP Client Secure Trustpoint	Trustpoint name.

Related Commands

Command	Description
http client secure-trustpoint	Declares the trustpoint that the HTTP client will use.
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.

show http client statistics

To display information about the communication between the HTTP server and the client, use the **show http client statistics** command in user EXEC or privileged EXEC mode.

show http client statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the data displayed by this command to determine whether the network topology between the HTTP server and client is properly designed and configured. To reset to zero all the counters that collect the information this command displays, use the **clear http client statistics** command.

Examples

The following sample output from this command shows statistics about the communication between the HTTP server and client:

```
Router# show http client statistics

    HTTP Client Statistics:
    =======================
Elapsed time: 759962960 msec

Load Count:
  total load count = 6899220
  total byte count = 26028731394
  largest file size = 624742 bytes
  smallest file size = 374 bytes

Server Response Time to Connect:
  longest response to connect = 10484 msec
  shortest response to connect = 24 msec

Server Response Time to Load:
  longest response to load = 11936 msec
  shortest response to load = 20 msec

File Load Time from Server:
  longest load time = 13124 msec
  shortest load time = 56 msec

Server Connection Count:
  max connections = 23
  established connections = 6901185
```

```
Load Rate:
  1 hour : 123300000 bytes
  1 min  : 2055000 bytes
  1 sec  : 34250 bytes
  1 msec : 34.25 bytes

Individual Counts:
  app_requests = 8538451                  app_callbacks = 8538451
  200_OK_rsp = 8512959                    other_rsp = 0
  total_errors = 25492                    client_timeouts = 25470
  client_errs = 0                         connect_errs/_timeouts = 7
  msg_decode_errs = 0                     msg_encode_errs = 0
  msg_xmit_errs = 15                      write_Q_full = 0
  socket_rcv_errs = 0                     supported_method_errs = 0
  retries = 4645                          late_responses = 0
  out_of_memory = 0                       mem_reallocs = 1206
  msg_malloced = 0                        event_malloced = 45
  cache_freed_by_ager = 1565
```

Table 116 describes the significant fields shown in the display.

Table 119 show http client statistics Field Descriptions

Field	Description
Elapsed time	Time elapsed since the first HTTP request, in milliseconds (ms).
total load count	Number of API events.
total byte count	Total bytes downloaded from the server by API requests.
largest file size smallest file size	Size of largest and smallest files downloaded from the server, in bytes.
longest response to connect shortest response to connect	Longest and shortest time taken by the server to establish a network connection requested by the client, in ms.
longest response to load shortest response to load	Longest and shortest time taken by the server to fulfill a download request from the client, in ms.
longest load time shortest load time	Longest and shortest time taken by the server to complete downloading the entire file, in ms.
max connections	Maximum concurrent connections.
established connections	Number of currently active and previously established connections.
Load Rate	Downloading rate in bytes/hour, bytes/minute, bytes/second, and bytes/ms.
app_requests	Number of GET and POST requests.
app_callbacks	Number of callbacks to the application.
200_OK_rsp	Number of server messages with response code 200 OK or 304 Not Modified.
other_rsp	Number of server messages with a response code other than 200 and 304.
total_errors	Number of errors encountered by the client.
client_timeouts	Number of timeouts the client has experienced, for example, response timeouts.
client_errs	Number of client internal errors, for example, software errors.

Table 119 show http client statistics Field Descriptions (continued)

Field	Description
connect_errs/_timeouts	Number of failed or broken connections.
msg_decode_errs	Number of server response messages for which the client failed to decode the headers.
msg_encode_errs	Number of send messages for which the client failed to encode the headers.
msg_xmit_errs	Number of send messages that the client failed to transmit to the server.
write_Q_full	Number of times that the client failed to enter a send message requested by an application into the transmit queue.
socket_rcv_errs	Number of socket read error events returned by TCP.
supported_method_errs	Number of unsupported methods requested by the application.
retries	Number of retransmitted messages.
late_responses	Number of messages that were decoded successfully but exceeded the timeout.
out_of_memory	Number of times that the client failed to allocate memory from Cisco IOS software.
mem_reallocs	Number of times that the client needed to readjust its buffer size because the server response message size exceeded the allocated buffer.
msg_malloced	Number of message buffers currently allocated for receiving messages from the server.
event_malloced	Number of event buffers currently allocated for application programming interface (API) requests.
cache_freed_by_ager	Number of HTTP client cache entries freed up by the background ager process.

Related Commands

Command	Description
clear http client statistics	Resets to zero all the counters that collect the information about the communication between the HTTP server and the client displayed in the output from the **show http client statistics** command.

show interface dspfarm

To display digital-signal-processor (DSP) information on the two-port T1/E1 high-density port adapter for the Cisco 7200 series, use the **show interface dspfarm** command in privileged EXEC mode.

show interface dspfarm [*slot*/*port*] **dsp** [*number*] [**long** | **short**]

Syntax Description

slot	(Optional) Slot location of the port adapter.
port	(Optional) Port number on the port adapter.
dsp	DSP information.
number	(Optional) Number of DSP sets to show. Range is from 1 to 30.
long	(Optional) Detailed DSP information.
short	(Optional) Brief DSP information.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

You can display the local time-division-multiplexing (TDM) cross-connect map by using the following form of this command: **show interface dspfarm <x/y | x/y/z> dsp tdm**..

Examples

The following is sample output from this command for port adapter slot 0 of chassis slot 3 on a Cisco 7200 series router:

```
Router# show interface dspfarm 3/0

DSPfarm3/0 is up, line protocol is up
  Hardware is VXC-2T1/E1
  MTU 256 bytes, BW 12000 Kbit, DLY 0 usec,
     reliability 255/255, txload 4/255, rxload 1/255
  Encapsulation VOICE, loopback not set
  C549 DSP Firmware Version:MajorRelease.MinorRelease (BuildNumber)
     DSP Boot Loader:255.255 (255)
     DSP Application:4.0 (3)
     Medium Complexity Application:3.2 (5)
     High Complexity Application:3.2 (5)
  Total DSPs 30, DSP0-DSP29, Jukebox DSP id 30
  Down DSPs:none
  Total sig channels 120 used 24, total voice channels 120 used 0
     0 active calls, 0 max active calls, 0 total calls
     30887 rx packets, 0 rx drops, 30921 tx packets, 0 tx frags
```

```
   0 curr_dsp_tx_queued, 29 max_dsp_tx_queued
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
5 minute input rate 13000 bits/sec, 94 packets/sec
5 minute output rate 193000 bits/sec, 94 packets/sec
   30887 packets input, 616516 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   30921 packets output, 7868892 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

Table 120 describes significant fields shown in this output.

Table 120 show interface dspfarm Field Descriptions

Field	Description
DSPfarm3/0 is up	DSPfarm interface is operating. The interface state can be up, down, or administratively down.
Line protocol is	Whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Version number of the hardware.
MTU	256 bytes.
BW	12000 kilobits.
DLY	Delay of the interface, in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability, calculated as an expediential average over 5 minutes).
Txload	Number of packets sent.
Rxload	Number of packets received.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Loopback conditions.
C549 DSP Firmware Version	Version of DSP firmware installed.
DSP Boot Loader	DSP boot loader version.
DSP Application	DSP application code version.
Medium Complexity Application	DSP Medium Complexity Application code version.
High Complexity Application	DSP High Complexity Application code version.
Total DSPs	Total DSPs that are equipped in the PA.
DSP0-DSP	DSP number range.
Jukebox DSP id	Jukebox DSP number.
Down DSPs	DSPs not in service.
Total sig channels...used...	Total number of signal channels used.
Total voice channels...used...	Total number of voice channels used.
Active calls	Number of active calls.

Table 120 show interface dspfarm Field Descriptions (continued)

Field	Description
Max active calls	Maximum number of active calls.
Total calls	Total number of calls.
Rx packets	Number of received (rx) packets.
Rx drops	Number of rx packets dropped at PA.
Tx packets	Number of transmit (tx) packets.
Tx frags	Number of tx packets that were fragmented.
Curr_dsp_tx_queued	Number of tx packets that are being queued at host DSP queues.
Max_dsp_tx_queued	The max total tx packets that were queued at host DSP queues.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output	Number of hours, minutes, and seconds since the last packet was successfully sent by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Last clearing of "show interface" counters	Number of times the "show interface" counters were cleared.
queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in output queue.
Drops	Number of packets dropped because of a full queue.
Input queue	Number of packets in input queue.
Minute input rate	Average number of bits and packets received per minute in the past 5 minutes.
Bits/sec	Average number of bits sent per second.
Packets/sec	Average number of packets sent per second.
Packets input	Total number of error-free packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
No buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.

Table 120 show interface dspfarm Field Descriptions (continued)

Field	Description
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Number of packets that are discarded because they exceed the maximum packet size for the medium. For instance, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Number of packet input errors.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
Overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
Ignore	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
Abort	Illegal sequence of one bits on the interface.
Packets output	Total number of messages sent by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Underruns	Number of times that the far end transmitter has been running faster than the near-end router's receiver can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this value might not balance with the sum of the enumerated output errors; some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.

Table 120 show interface dspfarm Field Descriptions (continued)

Field	Description
Collisions	Number of messages re-sent because of an Ethernet collision. Collisions are usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
Interface resets	Number of times an interface has been completely reset. Resetting can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurs, or when an interface is looped back or shut down.
Output buffer failures	Number of failed buffers.
Output buffers swapped out	Number of buffers swapped out.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces cable-modem

To display statistics for all interfaces configured on the cable modem port and to define Hybrid Fiber-Coax (HFC) statistics on the modem, use the **show interfaces cable-modem** command in privileged EXEC mode.

show interfaces cable-modem *port*

Syntax Description

port	The port number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command can be used to define the HFC state on the modem.

Examples

The following example shows the HFC state on the modem. The resulting output varies, depending on the network for which an interface has been configured.

```
Router# show interfaces cable-modem 0/1/0

cable-modem0/1/0 is up, line protocol is up
  HFC state is OPERATIONAL, HFC MAC address is 00d0.59e1.2073
  Hardware is Cable modem, address is 0014.f26d.10b2 (bia 0014.f26d.10b2)
  Internet address is 00.0.0.01/1
  MTU 1500 bytes, BW 1544 Kbit, DLY 6470 usec,
     reliability 255/255, txload 247/255, rxload 246/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:07:03
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 83594
  Queueing strategy: Class-based queueing
  Output queue: 61/1000/64/83594 (size/max total/threshold/drops)
     Conversations  2/5/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 232 kilobits/sec
  30 second input rate 2581000 bits/sec, 987 packets/sec
  30 second output rate 1585000 bits/sec, 639 packets/sec
  HFC input: 0 errors, 0 discards, 0 unknown protocols 0 flow control discards
  HFC output: 0 errors, 0 discards
     304582 packets input, 105339474 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 1 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     228195 packets output, 78392605 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
```

```
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Table 121describes the significant fields shown in the display.

Table 121 show interfaces cable-modem Field Descriptions

HFC State Values	Description
HFC state is OPERATIONAL	Current HFC state on the modem.
HFC MAC address	The HFC MAC address for this modem.
Hardware is Cable modem	Hardware type.
Internet address	The IP address for this modem.
MTU	Total MTU usage in bytes, kilobits, user seconds. Describes reliability, transmit load, and receiver load.
Encapsulation ARPA, loopback not set	Encapsulation type and whether loopback is set.
ARP type: ARPA, ARP Timeout	ARP type and timeout parameters.
Last input, output, output hang	Most recent input and output statistics.
Last clearing of “show interface” counters	Most recent usage of **show interface** command counters.
Input queue, Total output drops	Input queue and output drop statistics in the following format: size/max/drops/flushes.
Queueing strategy: Class-based queueing	Queueing type. In this case, class-based queueing.
Output queue	Output queue statistics in the following format: size/max total/threshold/drops.
Conversations	Type and number of conversations in the following format: active/max active/max total.
Reserved Conversations	Number of reserved conversations in the following format: allocated/max allocated.
Available Bandwidth	Allotted bandwidth in kilobits per second.
input rate, packets	Input rate and number of packets in bits per second, packets per second.
output rate, packets	Output rate and number of packets in bits per second, packets per second.
HFC input, output	HFC input statistics in the following format: errors, discards, unknown protocols, flow control discards.
packets input	Number of packets in bytes, with or without buffer.
Received broadcasts, runts, giants, throttles	Number of broadcasts, runts, giants, and throttles.
input errors	Number and type of input errors in the following format: cyclic redundancy check (CRC), frame, overrun, ignored.
packets output	Number of packets output in bytes and underruns.

Table 121 show interfaces cable-modem Field Descriptions (continued)

HFC State Values	Description
output errors, collisions, interface resets	Number of output errors, collisions, and interface resets.
babbles, late collision, deferred	Number of babbles, late collisions, and deferred packets.
lost carrier, no carrier	Carrier statistics.
output buffer failures, output buffers swapped out	Buffer statistics.

The HFC state is the Data Over Cable Service Interface Specification (DOCSIS) state for the cable modem connection to the cable modem termination system (CMTS). Table 122 describes HFC state values.

Table 122 HFC State Values

HFC State Values	Description
NOT_READY	Cable modem controller is resetting.
NOT_SYNCHRONIZED	Cable modem controller is starting the downstream frequency scan.
PHY_SYNCHRONIZED	Cable modem controller locked the downstream signal and is collecting the upstream channel parameter information.
US_PARAMETERS_ACQUIRED	Cable modem controller collected upstream channel parameter information and is trying to lock upstream frequency.
RANGING_COMPLETE	Cable modem controller received the CMTS range response, has finished downstream/upstream lock process, and is initializing IP.
IP_COMPLETE	Cable modem controller has IP information.
WAITING_FOR_DHCP_OFFER	Cable modem controller is sending a Dynamic Host Configuration Protocol (DHCP) request to the CMTS.
WAITING_FOR_DHCP_RESPONSE	Cable modem controller is waiting for a DHCP response from the CMTS.
WAITING_FOR_TIME_SERVER	Cable modem controller is starting the time of day (ToD) service.
TOD_ESTABLISHED	Cable modem controller has received the ToD packet and has synchronized its local time.
WAITING_FOR_TFTP	Cable modem controller is downloading its running configuration from the CMTS-defined TFTP server.
PARAM_TRANSFER_COMPLETE	Cable modem controller has completed transferring its running configuration.

Table 122 HFC State Values (continued)

HFC State Values	Description
REGISTRATION_COMPLETE	Cable modem controller has sent out its registration request, and CMTS has accepted it.
REFUSED_BY_CMTS	Cable modem controller registration request has been rejected by CMTS.
FORWARDING_DENIED	Cable modem controller registration to CMTS was successful, but network access is disabled in the running configuration.
OPERATIONAL	Cable modem controller is ready for service.
UNKNOWN	Cable modem controller is an undefined state

Table 123 lists input error descriptions.

Table 123 Input Error Description

Input Error	Description
errors	The total number of input packets discarded on the cable modem controller.
discards	The number of input packets discarded due to a momentary lack of resources.
unknown protocols	The number of input packets discarded because they have unsupported or unknown protocol values.
flow control discards	The number of input packets discarded because the cable modem controller overflowed transferring packets to the router.

Table 124 lists output error descriptions.

Table 124 Output Error Description

Output Error	Description
errors	Total number of output packets discarded on the cable modem controller.
discards	Total number of output packets discarded due to a momentary lack of resources.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces.

show iua as

To display information about the current condition of an application server (AS), use the **show iua as** command in privileged EXEC mode.

show iua as {**all** | **name** *as-name*}

Syntax Description

all	Output displays information about all configured ASs.
name *as-name*	Name of a particular AS. Output displays information about just that AS.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the **show iua as all** command to find the failover timer value. You need to know the current failover timer value before you changeit to fit your application.

Examples

The following sample output from this command shows that the current state of the AS (as1) is active and that there are four PRI interfaces configured to use this AS:

```
Router# show iua as all

Name of AS :as1
        Total num of ASPs configured :2
                asp1
                asp2
        Current state :  ACTIVE
        Active ASP :asp1
        Number of ASPs up :1
        Fail-Over time : 4000 milliseconds
        Local address list : 10.1.2.345 10.2.3.456
        Local port:2139
        Interface IDs registered with this AS
                 Interface ID
                 0 (Dchannel0)
                 3 (Dchannel3)
                 2 (Dchannel2)
                 1 (Dchannel1)
```

Table 125 describes significant fields shown in the output.

Table 125 show iua as all Field Descriptions

Field	Description
Name of AS: 1	Name of the AS.
Total num of ASPs configured :2 asp1 asp2	Total number of application server processes (ASPs) configured.
Current state : ACTIVE	The possible states are ACTIVE, INACTIVE, and DOWN.
Active ASP :asp1	Shows the active ASP.
Number of ASPs up :1	If two ASPs are up, then the one that is not active is in standby mode.
Fail-Over time : 4000 milliseconds	Default is 4000 ms, although the value can also be configured through the CLI under AS.
Local address list : 10.1.2.345 10.2.3.456	Configured by the user.
Local port:2139	Configured by the user.
Interface IDs registered with this AS Interface id 0 (Dchannel0) 3 (Dchannel3) 2 (Dchannel2) 1 (Dchannel1)	The D channels that are bound to this AS.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show isdn	Displays information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.
show iua asp	Displays information about the current condition of an ASP.

show iua asp

To display information about the current condition of an application server process (ASP), use the **show iua asp** command in privileged EXEC mode.

show iua asp {**all** | **name** *asp-name*}

Syntax Description

all	Displays information about all configured ASPs.
name *asp-name*	Name of a particular ASP. Displays information about just that ASP.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

This command establishes Stream Control Transmission Protocol (SCTP) associations. There can only be a maximum of two ASPs configured per application server (AS).

Examples

The following typical output for the **show iua asp all** command shows that the current state of the ASP (asp1) is active. This command also gives information about the SCTP association being used by this ASP.

```
Router# show iua asp all

Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc  id 0
SCTP Association information :
         Local Receive window :9000
         Remote Receive window :9000
         Primary Dest address requested by IUA 10.11.2.33
         Effective Primary Dest address 10.11.2.33
Remote  address list :10.22.3.44
Remote Port :9900
Statistics :
        Invalid SCTP signals Total :0  Since last  0
        SCTP Send failures :0
```

Table 126 describes significant fields shown in this output.

Table 126 show iua asp all Field Descriptions

Field	Description
Name of ASP: 1	Name of the application server process (ASP).
Current State of ASP: ASP-Active	The possible states are ACTIVE, INACTIVE, and DOWN.
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc id 0	States used for underlying SCTP association: IUA_ASSOC_ESTAB (association established) or IUA_ASSOC_INIT (association not established...attempting to initiate).
SCTP Association information : Local Receive window :9000 Remote Receive window :9000	Configured by the user.
Primary Dest address requested by IUA 10.11.2.33	The IP address through which the current link is established.
Remote address list :10.22.3.44 Remote Port :9900	Configured by the user.
Statistics : Invalid SCTP signals Total :0 Since last 0 SCTP Send failures :0	Information useful for seeing if errors are happening with the SCTP connection.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.

show media resource status

To display the current media resource status, use the **show media resource status** command in privileged EXEC mode.

show media resource status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example displays the current media resource status:

```
Router# show media resource status

 Resource Providers:

 Resource  Provider ID :: FLEX_DSPRM Status :: REGISTERED
 Service Profiles
 MTP ::
 TRANSCODING :: 6 11
 CONFERENCING :: 10
 Applications :
 Application ID : SCCP, Status : REGISTERED
```

Table 127 describes significant fields shown in this output.

Table 127 show media resource status Field Descriptions

Field	Description
MTP	Displays the profile numbers configured for MTP resources.
TRANSCODING	Displays the profile numbers configured for transcoding resources.
CONFERENCING	Displays the profile numbers configured for conferencing resources.
Status	Displays the current status of the profile.

Related Commands

Command	Description
dsp services dspfarm	Configures DSP farm services for a specified voice card.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show dspfarm profile	Displays configured DSP farm profile information for a Cisco CallManager group.

show mediacard

To display configuration information about media card conferencing, transcoding, Media Termination Points (MTPs) and Digital Signal Processors (DSPs), use the **show mediacard** command in privileged EXEC mode.

show mediacard slot [**conference** | **connections** | **dsp** *number*]

Syntax Description

slot	Specifies the slot number of the card to be displayed. Valid values are from 1 to 4.
conference	(Optional) Displays information on ad-hoc conferences.
connections	(Optional) Displays information on media card connections.
dsp *number*	(Optional) Displays information on the specified DSP resource pool. The *number* argument ranges in value from 1 to 4.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Use this command to display media card status, statistics, and configuration information.

Examples

The following is sample output for the **show mediacard** command:

```
Router# show mediacard 3

Media Card 3: WS-SVC-CMM-ACT
 Service: Adhoc/Meetme conference and MTP/Transcoding
 State: ENABLE
 DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 DSP status:
  DSP 1 | DSP 2 | DSP 3 | DSP 4
 -------|-------|-------|-------
  alive | alive | alive | alive
 Total 128 DSP channels, 1 active
 Resource pools                     | DSPs | Used by Active profile
 -----------------------------------|------|-----------------------
  Pool1                              |  2   |  1
  Pool2                              |  1   |
  Pool3                              |  1   |  2
```

```
Router# show mediacard 3 dsp 3

DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 Card DSP status Chan status RxPkts TxPkts
  3   3   alive  1    idle   -      -
                 2    idle   -      -
                 3    idle   -      -
                 4    idle   -      -
                 5    idle   -      -
                 6    idle   -      -
                 7    idle   -      -
                 8    idle   -      -
                 9    idle   -      -
                 10   idle   -      -
                 11   idle   -      -
                 12   idle   -      -
                 13   idle   -      -
                 14   idle   -      -
                 15   idle   -      -
                 16   idle   -      -
                 17   idle   -      -
                 18   idle   -      -
                 19   idle   -      -
                 20   idle   -      -
                 21   idle   -      -
                 22   idle   -      -
                 23   idle   -      -
                 24   idle   -      -
                 25   idle   -      -
                 26   idle   -      -
                 27   idle   -      -
                 28   idle   -      -
                 29   idle   -      -
                 30   idle   -      -
                 31   idle   -      -
                 32   idle   -      -
 Total 32 DSP channels, 0 active

Router# show mediacard conference

Id  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
    DSP/Ch
0   2/4/1 32024 16498   27004 27020  10.7.16.87
0   2/4/2 17368 17192   17582 17583  10.7.16.80
0   2/4/3 21904 16990   26155 26168 10.7.16.94
Total: 3

Router# show mediacard connections

Id  Type  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
          DSP/Ch
0   conf  3/4/1  24028 16552 0      0      10.7.16.87
Total: 1

Router# show mediacard connections

Id  Type  Slot/  RxPktsTxPktsRPort SPort Remote-Ip
          DSP/Ch
0   mtp   3/1/1  16544 16488 1046   1046   10.1.2.15
0   mtp   3/1/2  19396 19662 1046   1046   10.1.80.50
0   mtp   3/1/3  17562 20122 626    626    10.1.2.15
0   mtp   3/1/4  17488 17328 626    626    10.1.80.5
```

Table 128 describes the significant fields shown in the display.

Table 128 show mediacard Field Descriptions

Field	Description
RxPkts	Number of packets transmitted
TxPkts	Number of packets received
RPort	Receiving port
SPort	Sending port
Remote-Ip	IP address of the remote endpoint

Related Commands

Command	Description
debug mediacard	Displays debugging information for DSPRM.

show mgcp

To display values for Media Gateway Control Protocol (MGCP) parameters, use the **show mgcp** command in user EXEC or privileged EXEC mode.

show mgcp [**connection | endpoint | nas** {**dump** *slot port chan-number* **| info**} **| notify-entity | profile** [*name*] **| statistics**]

Syntax Description

connection	(Optional) Displays the active MGCP-controlled connections.
endpoint	(Optional) Displays the MGCP-controlled endpoints.
nas	(Optional) Displays Network Access Server (NAS) information.
dump	(Optional) Display MGCP data channel data.
slot	(Optional) Slot number.
port	(Optional) Port number.
chan-number	(Optional) Channel number.
info	(Optional) Displays MGCP data channel information.
notify-entity	(Optional) Displays MGCP notify entity information.
profile [*name*]	(Optional) Displays information about all the configured MGCP profiles. • *name*—Displays information about the specified MGCP profile.
statistics	(Optional) Displays MGCP statistics regarding received and transmitted network messages.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was modified. Command output was updated to display additional gateway and platform information.
12.1(5)XM	This command was modified. Command output was updated to display additional gateway and platform information.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(2)XA	This command was modified. The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	This command was modified. Command output was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB document *MGCP VoIP Call Admission Control*.) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(2)XN	This command was modified. Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200 routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. It was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5850, and Cisco IAD2420 series. The MGCP SGCP RSIP field was enhanced to show the status of the **mgcp sgcp disconnected notify** command.
12.2(13)T	This command was modified. Support was added for MGCP.
12.2(15)T	This command was implemented on Cisco 1751 and Cisco 1760 routers.
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26*xx*XM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37*xx* routers.
12.3(2)T	This command was implemented on the Cisco 26*xx*XM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37*xx* routers.
12.3(11)T	This command was modified. Command output was enhanced to display the enabled Secure Real-Time Transport Protocol (SRTP) package and enabled MGCP call-agent validation.
12.4(2)T	This command was modified. Command output was enhanced to display State Signaling Events (SSE) and Simple Packet Relay Transport (SPRT) configuration parameters.
12.4(11)T	This command was modified. The **show mgcp** command output was enhanced to display comedia-related configuration.
15.1(4)M	This command was integrated into Cisco IOS 15.1(4)M. The command output was enhanced to displays the configuration of the **tone-package** keyword in the MGCP- supported packages.

Usage Guidelines

This command provides high-level administrative information about the values configured for MGCP parameters on the router. For more specific information, use one of the optional keywords.

Use the **show mgcp** command to display SSE and SPRT parameters that have been configured to enable modem relay between IP secure telephone equipment (STE) and STE. The parameters are displayed only when the modem relay STE (mdste) package has been enabled using the **mgcp package-capability mdste-package** command.

Use the **show mgcp endpoint** command to display a list of MGCP endpoint responses when the configuring Media Gateway Control Protocol Basic Rate Interface Backhaul Signaling with Cisco CallManager feature.

The BRI endpoints are displayed in a similar manner to the way analog (Plain Old Telephone service) endpoints are displayed. The existing functions used for the analog endpoints are invoked. This display is independent of the platforms; hence the changes are required in the common code only.

This command checks for all the allocated “htsp_info_t” structures. These structures store information corresponding to all the endpoints. These structures are allocated only during system startup time. The structures are allocated for all the interfaces present, but the “vtsp_sdb_t” structure is allocated only for the first channel of the BRI port.

Since the endpoints that use the Media Gateway Control Protocol Application (MGCPAPP) as the application layer have to be displayed, the endpoints are displayed even if MGCPAPP is the only application being used by the endpoint. Because the MGCPAPP is shared across both the BRI channels and is port specific, both ports are displayed.

Examples

The following is partial sample output from the **show mgcp** command when the mdste modem relay package has been enabled:

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 3460 Initial protocol service is MGCP 0.1
MGCP validate call-agent source-ipaddr DISABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough disabled
MGCP voip nse modem relay: Disabled
MGCP voip mdste modem relay: Enabled
        SPRT rx v14 hold time: 50 (ms), SPRT tx v14 hold count: 16,
        SPRT tx v14 hold time: 20 (ms), SPRT Retries: 12
        SSE redundancy interval: 20 (ms), SSE redundancy packet: 3,
        SSE t1 timer: 1000 (ms), SSE retries: 3
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer: 5
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 20000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp ENABLED
MGCP undotted-notation DISABLED
```

```
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP Fax Playout Buffer is 300 in msec
MGCP media (RTP) dscp: ef, MGCP signaling dscp: af31
MGCP default package: line-package
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
                         line-package hs-package rtp-package script-package ms-package
                         dt-package mo-package mt-package sst-package mdr-package
                         fxr-package pre-package mdste-package srtp-package tone-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Max Fax Rate is DEFAULT
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
MGCP control bind :DISABLED
MGCP media bind :DISABLED
MGCP Upspeed payload type for G711ulaw: 0,  G711alaw: 8
MGCP Dynamic payload type for G.726-16K codec
MGCP Dynamic payload type for G.726-24K codec
MGCP Dynamic payload type for G.Clear codec
```

The following sample output displays the status of media source checking and the gateway role:

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.201 2497 Initial protocol service is MGCP 1.0
.
.
.
MGCP Dynamic payload type for NTE is 99
MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is PASSIVE
MGCP Comedia check media source is ENABLED
MGCP Comedia sdp force is DISABLED
MGCP Guaranteed scheduler time is DISABLED
MGCP DNS stale threshold is 30 seconds
.
.
.
```

The following is partial sample output from the **show mgcp** command when the mdste package has been disabled:

```
Router(config)# no mgcp package-capability mdste-package
Router(config)# exit
Router# show mgcp
MGCP voip mdste modem relay: Disabled
```

Table 129 describes the significant fields shown in the displays.

Table 129 show mgcp Field Descriptions

Field	Description
MGCP Admin State...Oper State	Administrative and operational state of the MGCP daemon. The administrative state controls the starting and the stopping of the application using the **mgcp** and **mgcp block-newcalls** commands. The operational state controls the normal MGCP operations.
MGCP call-agent	Address of the call agent specified in the **mgcp call-agent** or **call-agent** command and the protocol initiated for this session.
MGCP block-newcalls	State of the **mgcp block-newcalls** command.
MGCP send SGCP RSIP, disconnected	Setting for the **mgcp sgcp restart notify** and the **mgcp sgcp disconnected notify** commands (enabled or disabled).
MGCP quarantine mode	How the quarantine buffer is to handle Simple Gateway Control Protocol (SGCP) events.
MGCP quarantine of persistent events is	Specifies whether the SGCP persistent events are handled by the quarantine buffer.
MGCP dtmf-relay	Setting for the **mgcp dtmf-relay** command.
MGCP voip modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode**, **mgcp modem passthrough codec**, and **mgcp modem passthrough voip redundancy** commands.
MGCP voip mdste modem relay	Settings for the **mgcp modem relay voip sprt v14 receive playback**, **mgcp modem relay voip sprt v14 transmit maximum hold-count**, **mgcp modem relay voip sprt v14 transmit hold-time**, **mgcp modem relay voip sprt retries**, **mgcp modem relay voip sse redundancy**, and **mgcp modem relay voip sse t1** commands.
SPRT rx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 receive playback hold-time** *time* command.
SPRT tx v14 hold count	Setting for the **mgcp modem relay voip sprt v14transmit maximum hold-count** *characters* command.
SPRT tx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 transmit hold-time** *time* command.
SPRT Retries	Setting for the **mgcp modem relay voip sprt retries** command.
SSE redundancy interval	Setting for the **mgcp modem relay voip mode sse redundancy interval** *time* command.
SSE redundancy packet	Setting for the **mgcp modem relay voip mode sse redundancy packet** command.
SSE t1 timer	Setting for the **mgcp modem relay voip mode sse redundancy t1** command.
SSE retries	Setting for the **mgcp modem relay voip mode sse redundancy retries** command.

Table 129 show mgcp Field Descriptions (continued)

Field	Description
MGCP Comedia role	Location of gateway: • **ACTIVE**—inside NAT • **PASSIVE**—outside NAT
MGCP Comedia check media source	Global media IP and port address detection status (ENABLED or DISABLED).
MGCP Comedia sdp force	Configuration state of forced insertion of the direction attribute in the SDP (ENABLED or DISABLED)
MGCP TSE payload	Setting for the **mgcp tse payload** command.
MGCP Network (IP/AAL2) Continuity Test timer	Setting for the **net-cont-test** keyword in the **mgcp timer** command.
MGCP 'RTP stream loss' timer	Setting for the **receive-rtcp** keyword in the **mgcp timer** command.
MGCP request timeout	Setting for the **mgcp request timeout** command.
MGCP maximum exponential request timeout	Setting for the **mgcp request timeout max** command.
MGCP gateway port	UDP port specification for the gateway.
MGCP maximum waiting delay	Setting for the **mgcp max-waiting-delay** command.
MGCP restart delay	Setting for the **mgcp restart-delay** command.
MGCP vad	Setting for the **mgcp vad** command.
MGCP rtrcac	Specifies whether MGCP SA Agent CAC has been enabled with the **mgcp rtrcac** command.
MGCP system resource check	Specifies whether MGCP SRC CAC has been enabled with the **mgcp src-cac** command.
MGCP xpc-codec	Specifies whether the **mgcp sdp xpc-codec** command has been configured to generate the X-pc codec field for Session Description Protocol (SDP) codec negotiation in Network-Based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).
MGCP persistent hookflash	Specifies whether the **mgcp persistent hookflash** command has been configured to send persistent hookflash events to the call agent.
MGCP persistent offhook	Specifies whether the **mgcp persistent offhook** command has been configured to send persistent off-hook events to the call agent.
MGCP persistent onhook	Specifies whether the **mgcp persistent onhook** command has been configured to send persistent on-hook events to the call agent.
MGCP piggyback msg	Specifies whether the **mgcp piggyback message** command has been configured to enable piggyback messaging.
MGCP endpoint offset	Specifies whether the **mgcp endpoint offset** command has been configured to enable incrementing of the local portion of an endpoint name for NCS. The local portion contains the analog or digital voice port identifier.
MGCP simple-sdp	Specifies whether the **mgcp sdp simple** command has been configured to enable simple mode SDP operation.

Table 129 show mgcp Field Descriptions (continued)

Field	Description
MGCP undotted-notation	Specifies whether the **mgcp sdp notation undotted** command has been configured to enable undotted SDP notation for the codec string.
MGCP codec type	Setting for the **mgcp codec** command.
MGCP packetization period	The **packetization period** parameter setting for the **mgcp codec** command.
MGCP JB threshold lwm	Jitter-buffer minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP JB threshold hwm	Jitter-buffer maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold lwm	Latency minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold hwm	Latency maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold lwm	Packet-loss minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold hwm	Packet-loss maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP CL threshold lwm	Cell-loss minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP CL threshold hwm	Cell-loss maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP playout mode is	Jitter-buffer packet type and size.
MGCP default package	Package configured as the default package with the **mgcp default-package** command.
MGCP supported packages	Packages configured with the **mgcp package-capability** command to be supported on this gateway in this session. The Line Control Signaling Package (lcs-package) display is new in Cisco IOS Release 12.3(8)T.
MGCP voaal2 modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode** and **mgcp modem passthrough codec** commands.
MGCP T.38 Fax	Settings for the **mgcp fax t.38** command. The following values are displayed: • MGCP T.38 fax: ENABLED or DISABLED. • Error correction mode (ECM): ENABLED or DISABLED. • Nonstandard facilities (NSF) override: ENABLED or DISABLED. If enabled, the override code is displayed. • MGCP T.38 fax low-speed redundancy: the factor set on the gateway for redundancy. • MGCP T.38 fax high-speed redundancy: the factor set on the gateway for redundancy.

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
isdn bind-l3 (interface BRI)	Configures the BRI to support MGCP and to bind ISDN Layer 3 with Cisco CallManager backhaul.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables IP address and port detection from the first RTP packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
mgcp package-capability mdste-package	Specifies the MGCP package capability type for a media gateway.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show ccm-manager	Displays a list of Cisco CallManager servers and their current statuses, and availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp connection

To display information for active connections that are controlled by the Media Gateway Control Protocol (MGCP), use the **show mgcp connection** command in privileged EXEC mode.

show mgcp connection

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control*.) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(11)T	Command output was enhanced to display the encryption suite used on the Secure Real-Time Transport Protocol (SRTP) connection.

Release	Modification
12.4(2)T	Command output was enhanced to display the current media state.
12.4(11)T	Command output was enhanced to display the detected NAT address and port.

Examples

The following is sample output from the **show mgcp connection** command displaying a secure call for which the media state is modem relay mode:

```
Router# show mgcp connection

Endpoint  Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
(ME)dia
1. S2/DS1-2/1   C=A0000000010000010000000F5,4,3  I=0x2  P=17098,2662  M=3 S=4,4 CO=1
E=3,0,0,3  R=0,0  ME=2
```

The following is sample output from this command showing the detected NAT address and port. The (P)ort output shows the local and advertised ports prior to detection. The (COM)Addr/Port output shows the detected media address and port (10.7.1.21:1500):

```
Router# show mgcp connection

Endpoint   Call_ID(C) Conn_ID (I) (P)ort (M)ode(S)tate(CO)dec (E)vent[SIFL] (R)esult[EA]
(COM)Addr/Port
S7/DS1-4/1 C=201597,768784,768785 I=0x5DD85 P=18258,19062 M=3 S=4,4 CO=2 E=2,0,0,2
R=0,0,0,2 COM=10.7.1.21:15000
```

The following is sample output from this command for encrypted connections:

```
Router# show mgcp connection

Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL]
(R)esult[EA] Encryption(K)
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1
```

The following is sample output from this command for VoIP connections:

```
Router# show mgcp connection

Endpoint   Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0

Total number of active calls 6
```

The following is sample output from this command for Voice over ATM Adaptation Layer 2 (VoAAL2) connections:

```
Router# show mgcp connection

Endpoint  Call_ID(C) Conn_ID(I)(V)cci/cid (M)ode (S)tate (C)odec (E)vent[SIFL]
(R)esult[EA]
1.aaln/S1/1   C=1,11,12    I=0x2    V=2/10     M=3    S=4,4    C=1    E=3,0,0,3     R=0,0

Total number of active calls 1
```

Table 130 describes the significant fields shown in the displays.

Table 130 show mgcp connection Field Descriptions

Field	Description
Endpoint	Endpoint for each call shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call_ID(C)	MGCP call ID sent by the call agent, the internal Call Control Application Programming Interface (CCAPI) call ID for this endpoint, and the CCAPI call ID of the peer call legs. (CCAPI is an API that provides call control facilities to applications.)
(COM)Addr/Port	Detected media address and port.
Conn_ID(I)	Connection ID generated by the gateway and sent in the ACK message.
(P)ort	Ports used for this connection. The first port is the local User Datagram Protocol (UDP) port. The second port is the remote UDP port.
(V)cci/cid	Virtual channel connection identifier (VCCI) and channel identifier (CID) used for the VoAAL2 call.
(Me)dia	Media state, where: • 0—Voice • 1—Modem pass-through • 2—Modem relay
(M)ode	Call mode, where: • 0—Invalid value for mode. • 1—Gateway should only send packets. • 2—Gateway should only receive packets. • 3—Gateway should send and receive packets. • 4—Gateway should neither send nor receive packets. • 5—Gateway should place the circuit in loopback mode. • 6—Gateway should place the circuit in test mode. • 7—Gateway should use the circuit for network access for data. • 8—Gateway should place the connection in network loopback mode. • 9—Gateway should place the connection in network continuity test mode. • 10—Gateway should place the connection in conference mode. All other values are used for internal debugging.
(S)tate	Call state. The values are used for internal debugging purposes.
(Co)dec	Codec identifier. The values are used for internal debugging purposes.
(E)vent [SIFL]	Used for internal debugging.
(R)esult [EA]	Used for internal debugging.

Table 130 show mgcp connection Field Descriptions

Field	Description
Encryption(K)	Encryption suite, where: • 0—None • 1—AES_CM_128_HMAC_SHA1_32

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays values for MGCP parameters.
show mgcp endpoints	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp endpoint

To display information for endpoints controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp endpoint** command in privileged EXEC mode.

show mgcp endpoint

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	The output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following is sample output from this command:

```
Router# show mgcp endpoint

       ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-0/1@nytnk116      0:1    fxs-gs     up
     ds1-0/2@nytnk116      0:1    fxs-gs     up
     ds1-0/3@nytnk116      0:1    fxs-gs     up
     ds1-0/4@nytnk116      0:1    fxs-gs     up
     ds1-0/5@nytnk116      0:1    fxs-gs     up
     ds1-0/6@nytnk116      0:1    fxs-gs     up
     ds1-0/7@nytnk116      0:1    fxs-gs     up
     ds1-0/8@nytnk116      0:1    fxs-gs     up
     ds1-0/9@nytnk116      0:1    fxs-gs     up
    ds1-0/10@nytnk116      0:1    fxs-gs     up
    ds1-0/11@nytnk116      0:1    fxs-gs     up
    ds1-0/12@nytnk116      0:1    fxs-gs     up
    ds1-0/13@nytnk116      0:1    fxs-gs     up
    ds1-0/14@nytnk116      0:1    fxs-gs     up
    ds1-0/15@nytnk116      0:1    fxs-gs     up
    ds1-0/16@nytnk116      0:1    fxs-gs     up
    ds1-0/17@nytnk116      0:1    fxs-gs     up
    ds1-0/18@nytnk116      0:1    fxs-gs     up
    ds1-0/19@nytnk116      0:1    fxs-gs     up
    ds1-0/20@nytnk116      0:1    fxs-gs     up
    ds1-0/21@nytnk116      0:1    fxs-gs     up
    ds1-0/22@nytnk116      0:1    fxs-gs     up
    ds1-0/23@nytnk116      0:1    fxs-gs     up
    ds1-0/24@nytnk116      0:1    fxs-gs     up

Interface T1 1

        ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-1/1@nytnk116      1:1    e&m-imd    up
     ds1-1/2@nytnk116      1:1    e&m-imd    up
```

Table 131 describes significant fields shown in this output.

Table 131 show mgcp endpoint Field Descriptions

Field	Description
ENDPOINT-NAME	Name used by the call agent to identify a specific mgcp endpoint on a given gateway.
V-PORT	Voice port
SIG-TYPE	Signaling type for a given endpoint (for example, NONE for SS7 ISDN User Part (ISUP) and FXS-GS for Foreign Exchange Station (FXS) Ground Start).
ADMIN	Administrative status—Up or Down. (This field is populated only on residential gateway (RGW) platforms.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.

Command	Description
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp nas

To display Media Gateway Control Protocol (MGCP) network access server (NAS) information for data ports, use the **show mgcp nas** command in privileged EXEC mode.

show mgcp nas {**dump** *slot port channel* | **info**}

Syntax Description

dump *slot port channel*	Displays NAS information for the specified port and channel. The arguments are as follows: • *slot*—Chassis slot for interface card. Values are as follows: – Cisco AS5350: From 0 to 3. – Cisco AS5400: From 0 to 7. – Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC). • *port*—Modem interface port. Values are as follows: – Cisco AS5350: For T1/E1, from 0 to 7. For T3, from 1 to 28. – Cisco AS5400: For T1/E1, from 0 to 7. For T3, from 1 to 28. – Cisco AS5850: For T1/E1, from 0 to 23. For T3, from 1 to 28. • *channel*—T1 or E1 channel. Values for T1 are from 1 to 24. Values for E1 are from 1 to 31.
info	Displays status of NAS channels.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	The output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(7)YB	The valid values for the bearer cap field of the **show mgcp nas dump** command output were changed to include LAPB, V.120, and sync data. The Signaling field was added to the **show mgcp nas dump** command output. See Table 132.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T

Examples

The following is sample output from this command for an autodetected V.120 call:

```
Router# show mgcp nas dump 1 7 24

Slot 1 state=Up
Port 7 state=Up
State In Use PortCb=0x6577949C ss_id=0x0 handle=0x65C88228
Bearer Cap=V.120 call_id=1 conn_id=6577B8EC
Sig Type=Autodetect
Events req- nas/crq- req id=7 :nas/of- req id=7 :
Endpt name=S1/DS1-7/24
call_id = 1, conn_id=0x6577B8EC cgn=1000 cdn=5555
Rx packets=610  Rx bytes=73242 Tx packets 716 Tx bytes 72987
```

Table 132 describes the significant fields shown in the display.

Table 132 show mgcp nas dump Field Descriptions

Field	Description
Slot state	Status of specified slot.
Port state	Status of specified port.
State	Call status for the specified channel.
bearer cap	Bearer capability. Values are: • Modem • LAPB • V.110 • V.120 • Digital 64 • Digital 56 V.110, V.120, modem, or digital values are displayed when autodetection is not enabled and the signaling type is set to External. LAPB, V.120, and digital values are displayed if autodetection is enabled, and the signaling type is set to Autodetect.
call_id	Call identification for the currently active call, if any.
conn_id	Connection identification for the currently active call, if any.
Signaling	Call type signaling. Values are: • External—Call type is signaled by the call agent. • Autodetect—Call type is autodetected by the gateway.
Events req	List of NAS events requested, if any, and their request IDs. The request ID identifies the MGCP message from the call agent that requested the events.
Endpt name	MGCP endpoint name.

The following sample output from this command shows the state, either Idle or In Use, for each channel:

```
Router# show mgcp nas info

Number of ports configured=1
Slot 1 configured  slot state=Up  Port 7 state=Up
=====Port 7 Channel States=====
 0  Idle
 1  Idle
 2  Idle
 3  Idle
 4  Idle
 5  Idle
 6  Idle
 7  Idle
 8  Idle
 9  Idle
 10 Idle
 11 Idle
 12 Idle
 13 Idle
```

```
 14 Idle
 15 Idle
 16 Idle
 17 Idle
 18 Idle
 19 Idle
 20 Idle
 21 Idle
 22 Idle
 23 In Use
=====================================
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp profile

To display information for Media Gateway Control Protocol (MGCP) profiles, use the **show mgcp profile** command in privileged EXEC mode.

show mgcp profile [*profile-name*]

Syntax Description

profile-name	(Optional) Name of the MGCP profile for which information should be displayed; limited to 32 characters.

Command Default

If the optional *profile-name* argument is not used, all configured profiles are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Release	Modification
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.4(4)T	Output was added to show the order in which ANI and DNIS digits are sent to the call agent.

Examples

The following is sample output for this command for the default profile:

```
Router# show mgcp profile default

MGCP Profile default
Description: None
Call-agent: none Initial protocol service is unknown
Tsmax timeout is 20 sec, Tdinit timeout is 15 sec
Tdmin timeout is 15 sec, Tdmax timeout is 600 sec
Tcrit timeout is 4 sec, Tpar timeout is 16 sec
Thist timeout is 30 sec, MWI timeout is 16 sec
Ringback tone timeout is 180 sec, Ringback tone on connection timeout is 180 sec
Network congestion tone timeout is 180 sec, Busy tone timeout is 30 sec
Dial tone timeout is 16 sec, Stutter dial tone timeout is 16 sec
Ringing tone timeout is 180 sec, Distinctive ringing tone timeout is 180 sec
Continuity1 tone timeout is 3 sec, Continuity2 tone timeout is 3 sec
Reorder tone timeout is 30 sec,  Persistent package is ms-package
Max1 DNS lookup: ENABLED, Max1 retries is 5
Max2 DNS lookup: ENABLED, Max2 retries is 7
Source Interface: NONE
T3 endpoint naming convention is T1
CAS Notification Digit order is DNIS-ANI
```

The following is sample output for this command for a profile named “example”*:*

```
Router# show mgcp profile example

MGCP Profile example
Description:None
Call-agent:10.9.57.6 5003 Initial protocol service is MGCP 1.0
Tsmax timeout is 20, Tdinit timeout is 15
Tdmin timeout is 15, Tdmax timeout is 600
Tcrit timeout is 4, Tpar timeout is 16
Thist timeout is 30, MWI timeout is 16
Ringback tone timeout is 180, Ringback tone on connection timeout is 180
Network congestion tone timeout is 180, Busy tone timeout is 30
Dial tone timeout is 16, Stutter dial tone timeout is 16
Ringing tone timeout is 180, Distinctive ringing tone timeout is 180
Continuity1 tone timeout is 3, Continuity2 tone timeout is 3
Reorder tone timeout is 30,  Persistent package is ms-package
Max1 DNS lookup:ENABLED, Max1 retries is 4
Max2 DNS lookup:ENABLED, Max2 retries is 6
Voice port:1
```

Table 133 describes significant fields shown in these outputs.

Table 133 show mgcp profile Field Descriptions

Field	Description
MGCP Profile	The name configured for this profile with the **mgcp profile** command.
Description	Description configured for this profile with the **description MGCP profile** command.
Call-agent	Domain name server (DNS) or IP address of the call agent, as configured for this profile with the **call-agent** command.
Initial protocol service	Protocol service to be used, as configured for this profile with the **call-agent** command.
Tsmax timeout	Maximum timeout value for removing messages from the retransmission queue, as configured for this profile by the **timeout tsmax** command.
Tdinit timeout	Initial waiting delay, as configured for this profile by the **timeout tdinit** command.
Tdmin timeout	Minimum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmin** command.
Tdmax timeout	Maximum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmax** command.
Tcrit timeout	Critical timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tcrit** command.
Tpar timeout	Partial timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tpar** command.
Thist timeout	Packet storage timeout value, as configured for this profile by the **timeout thist** command.
MWI timeout	Timeout value for message-waiting-indicator tone, as configured for this profile by the **timeout tone mwi** command.
Ringback tone timeout	Timeout value for ringback tone, as configured for this profile by the **timeout tone ringback** command.
Ringback tone on connection timeout	Timeout value for ringback tone on connection, as configured for this profile by the **timeout tone ringback connection** command.
Network congestion tone timeout	Timeout value for the network congestion tone, as configured for this profile by the **timeout tone network congestion** command.
Busy tone timeout	Timeout value for the busy tone, as configured for this profile by the **timeout tone busy** command.
Dial tone timeout	Timeout value for the dial tone, as configured for this profile by the **timeout tone dial** command.
Stutter dial tone timeout	Timeout value for the stutter dial tone, as configured for this profile by the **timeout tone dial stutter** command.
Ringing tone timeout	Timeout value for the ringing tone, as configured for this profile by the **timeout tone ringing** command.
Distinctive ringing tone timeout	Timeout value for the distinctive ringing tone, as configured for this profile by the **timeout tone ringing distinctive** command.

Table 133 show mgcp profile Field Descriptions (continued)

Field	Description
Continuity1 tone timeout	Timeout value for the continuity1 tone, as configured for this profile by the **timeout tone cot1** command.
Continuity2 tone timeout	Timeout value for the continuity2 tone, as configured for this profile by the **timeout tone cot2** command.
Reorder tone timeout	Timeout value for the reorder tone, as configured for this profile by the **timeout tone reorder** command.
Persistent package	Name of package configured as persistent for this profile by the **package persistent** command.
Max1 lookup	Domain name server (DNS) lookup for the call agent after the suspicion threshold is reached, as configured for this profile by the **max1 lookup** command.
Max1 retries	Number of retries to reach the call agent before a new DNS lookup is performed, as configured for this profile by the **max1 retries** command.
Max2 lookup	DNS lookup for the call agent after the disconnected threshold is reached, as configured by the **max2 lookup** command.
Max2 retries	Maximum number of retries to reach the call agent before a new DNS lookup is performed, as configured by the **max2 retries** command.
CAS Notification Digit order	Order in which ANI and DNIS digits are sent in the notify message as configured with the **notify** command.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by the gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp srtp

To display information for active Secure Real-Time Transport Protocol (SRTP) connections that are controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp srtp** command in privileged EXEC mode.

show mgcp srtp {**summary** | **detail** [*endpoint*]}

Syntax Description

summary	Displays MGCP SRTP connections summary.
detail *endpoint*	Displays MGCP SRTP connections details. • The *endpoint* argument allows you to limit the display to endpoints for a specific connection. The *endpoint* argument can take the following values: – Port numbers. – The asterisk wildcard character *.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command provides information about secure calls created by the MGCP application. To specify connection endpoints for display, use the **show mgcp srtp detail endpoint** command. To display valid values for the *endpoint* argument, that is, the endpoint port numbers, use the **show mgcp connection** command. Use the **show mgcp srtp detail** command to display a hashed version of the master key and salts (encryption mechanisms) used on each connection. This display allows you to validate keys and salts for each endpoint of a call without revealing the actual master key and salt.

Examples

The following is sample output from this command for encrypted connections:

```
Router# show mgcp srtp summary

MGCP SRTP Connection Summary
Endpoint              Conn Id    Crypto Suite
aaln/S3/SU0/0         8          AES_CM_128_HMAC_SHA1_32
aaln/S3/SU0/1         9          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/1            6          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/2            7          AES_CM_128_HMAC_SHA1_32

4 SRTP connections active
```

```
Router# show mgcp srtp detail

MGCP SRTP Connection Detail for Endpoint *


Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source,
ROC=Rollover Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order,
MLT=Master Key Lifetime, MKI=Master Key Index:MKI Size

Endpoint aaln/S3/SU0/0 Call ID 2 Conn ID 8
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

Endpoint aaln/S3/SU0/1 Call ID 101 Conn ID 9
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured

Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured

4 SRTP connections displayed

Router# show mgcp srtp detail S3/DS1-0/*

MGCP SRTP Connection Detail for Endpoint S3/DS1-0/*

Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source,
ROC=Rollover Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order,
MLT=Master Key Lifetime, MKI=Master Key Index:MKI Size

Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured

2 SRTP connections displayed
```

Table 134 describes the significant fields shown in the display.

Table 134 show mgcp srtp Field Descriptions

Field	Description
Endpoint	Endpoint for each call, shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call ID	MGCP call ID sent by the call agent.
Conn ID	Connection ID generated by the gateway and sent in the ACK message.
Crypto Suite	Identifies the cryptographic suite used on the connection.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays values for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.

show mgcp statistics

To display Media Gateway Control Protocol (MGCP) statistics regarding received and transmitted network messages, use the **show mgcp statistics** command in privileged EXEC mode.

show mgcp statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp** command was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service assurance agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2)XB online document *MGCP VoIP Call Admission Control.*) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. To simplify the command reference, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(11)T	Output was enhanced to display dropped packets from unconfigured call agents if call-agent validation is enabled.

Examples

The following is sample output from this command for VoIP and VoAAL2 statistics:

```
Router# show mgcp statistics

UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
Rx packets from unknown Call Agent 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```

The following is an example of the MGCP VoIP SRC CAC portion of this command output for a gateway configured with MGCP VoIP SRC CAC:

```
Router# show mgcp statistics

MGCP System Resource Check Statistics:
-------------------------------------
Total CreateConn checked by SRC :0
CreateConn accepted by SRC:0
CreateConn rejected by SRC:0
Total ModifyConn checked by SRC :0
ModifyConn accepted by SRC:0
ModifyConn rejected by SRC:0
Reason          Num. of requests rejected
------          -------------------------
cpu-5sec:       0
cpu-avg:        0
total-mem:      0
io-mem:         0
proc-mem:       0
total-calls:    0
```

Table 135 describes significant fields shown in this output.

Table 135 show mgcp statistics Field Descriptions

Field	Description
UDP pkts rx, tx	Number of User Datagram Protocol (UDP) packets transmitted and received from the call agent by the gateway MGCP application.
Unrecognized rx pkts	Number of unrecognized UDP packets received by the MGCP application.
MGCP message parsing errors	Number of MGCP messages received with parsing errors.
Duplicate MGCP ack tx	Number of duplicate MGCP acknowledgment messages transmitted to the call agents.
Invalid versions count	Number of MGCP messages received with invalid MGCP protocol versions.

Table 135 show mgcp statistics Field Descriptions (continued)

Field	Description
Rx packets from unknown Call Agent	Number of dropped packets from unconfigured call agents.
CreateConn rx	Number of Create Connection (CRCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn rx	Number of Delete Connection (DLCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn tx	Number of DLCX messages sent from the gateway to the call agent (CA).
ModifyConn rx	Number of Modify Connection (MDCX) messages received by the gateway, the number that were successful, and the number that failed.
NotifyRequest rx	Number of Notify Request (RQNT) messages received by the gateway, the number that were successful, and the number that failed.
AuditConnection rx	Number of Audit Connection (AUCX) messages received by the gateway, the number that were successful, and the number that failed.
AuditEndpoint rx	Number of Audit Endpoint (AUEP) messages received by the gateway, the number that were successful, and the number that failed.
RestartInProgress tx	Number of Restart in Progress (RSIP) messages sent by the gateway, the number that were successful, and the number that failed.
Notify tx	Number of Notify (NTFY) messages sent by the gateway, the number that were successful, and the number that failed.
ACK tx, NACK tx	Number of Acknowledgment and Negative Acknowledgment messages sent by the gateway.
ACK rx, NACK rx	Number of Acknowledgment and Negative Acknowledgment messages received by the gateway.
IP address based Call Agents statistics: IP address, Total msg rx	IP address of the call agent, the total number of MGCP messages received from that call agent, the number of messages that were successful, and the number of messages that failed.
Total CreateConn checked by SRC	Total number of Create Connection (CRCX) messages that have been checked against the SRC component.
CreateConn accepted by SRC	Number of CRCX messages that have been accepted after being checked by the SRC component.
CreateConn rejected by SRC	Number of CRCX messages that have been rejected by SRC because of resource constraints.
Total ModifyConn checked by SRC	Total number of Modify Connection (MDCX) messages that have been checked against the SRC component.

Table 135 show mgcp statistics Field Descriptions (continued)

Field	Description
ModifyConn accepted by SRC	Number of MDCX messages that have been accepted after being checked by the SRC component.
ModifyConn rejected by SRC	Number of MDCX messages that have been rejected by SRC because of resource constraints.
Reason	Specific threshold that was exceeded to cause the rejection.
Num. of requests rejected	Number of requests that have been rejected.
cpu-5sec	CPU utilization for previous 5 seconds threshold was exceeded.
cpu-avg	Average CPU utilization threshold was exceeded.
total-mem	Total memory utilization threshold was exceeded.
io-mem	I/O memory utilization threshold was exceeded.
proc-mem	Processor memory utilization threshold was exceeded.
total-calls	Total number of calls threshold was exceeded.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.

show modem relay statistics

To display various statistics for modem relay, use the **show modem relay statistics** command in privileged EXEC mode.

show modem relay statistics {**all** | **phy** | **pkt** | **queue** | **sprt** | **timer** | **v14** | **v42**} [**call-identifier** *call-setup-time call-index*]

Syntax Description

all	All statistics associated with the modem-relay feature.
phy	Modem-relay physical layer statistics.
pkt	Modem-relay packetizer statistics.
queue	Modem-relay queue statistics.
sprt	Modem-relay SPRT layer statistics.
timer	Modem-relay timer statistics.
v14	Modem-relay V.14 statistics
v42	Modem-relay V.42 statistics.
call-identifier *call-setup-time*	(Optional) Value of the system UpTime when the call that is associated with this entry was started. Range is from 0 to 4294967295.
call-identifier *call-index*	(Optional) Dial-peer identification number used to distinguish between calls with the same setup time. Range is from 0 to 4294967295.

Command Default

No statistics are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 7200 series, and Cisco AS5300.
12.4(2)T	The **v14** keyword was added.

Usage Guidelines

Use this command to display various modem-relay call statistics, including counts of different types of packets, errors, and events, for all modem-relay calls.

Display statistics for a specific modem-relay call by using the **call-identifier** keyword and specifying the call-setup time and call index of the desired call. Obtain values for the call-setup time and call index from the SetupTime and Index fields at the start of each call record in the **show call active** command output.

Examples

The following is sample output from the **show modem relay statistics v14** command:

```
Router# show modem relay statistics v14

ID:11D6

V14 Layer Statistics
           sync_count=47 sync_loss_count=46
           min_bundle_size_rcvd_local=1 max_bundle_size_rcvd_local=20
           min_bundle_size_rcvd_remote=0 max_bundle_size_rcvd_remote=0
           info_bytes_removed_dueto_phy_rcv_q=0
           overflow_count_rcv_q=0
           info_bytes_removed_dueto_old_age_rcv_q=0
           info_bytes_discarded_bad_offset_rcv_q=0
           info_bytes_overwrite_rcv_q=0
           info_bytes_filled_rcv_q=0
           total_bytes_rcv_local=310
           min_bundle_size_send_local=0, max_bundle_size_send_local=0
           min_bundle_size_send_network=1, max_bundle_size_send_network=22
           info_bytes_removed_dueto_phy_xmit_q=0, overflow_count_xmit_q=0
           info_bytes_discarded_bad_offset_xmit_q=0
           info_bytes_overwrite_xmit_q=0
           info_bytes_filled_xmit_q=0, total_bytes_xmit_local=0

           Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics all call-identifier 43009 1

ID:3

SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=122
        sprt_tc2_explicit_acks_rcvd=126 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=129 sprt_tc2_explicit_acks_sent=132
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=289 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500

Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0

V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1385 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=1374 v42_rcvd_rnr=0 v42_rcvd_rej=0
```

```
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1464 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0

Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0

Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1385
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0

Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1333
```

The following is sample output from this command:

```
Router# show modem relay statistics all

ID:3

SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=155
        sprt_tc2_explicit_acks_rcvd=158 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=161 sprt_tc2_explicit_acks_sent=165
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=357 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500

Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0

V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1910 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
```

```
        v42_rcvd_rr=1899 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1988 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0

Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0

Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1910
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0

Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1809

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics sprt

ID:3

SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=177
        sprt_tc2_explicit_acks_rcvd=180 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=183 sprt_tc2_explicit_acks_sent=187
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=403 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics queue

ID:3

Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics v42

ID:3

V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=2442 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=2431 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=2539 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics phy

ID:3

Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat pkt

ID:3

Packetizer Statistics
        frames_inprogress=5 good_crc_frames=2573
        bad_crc_frames=61 frame_aborts=150
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0

        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat timer

ID:3

Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=2750

        Total Modem Relay Call Legs = 1
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
show call active	Displays active call information for voice calls or fax transmissions in progress.
show call active voice	Displays current call information for a call in progress.
show modems	Displays all modem configurations.

show mrcp client session active

To display information about active Media Resource Control Protocol (MRCP) client sessions, use the **show mrcp client session active** command in privileged EXEC mode.

show mrcp client session active [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each active MRCP session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version, ASR callid, and TTS callid fields were added to the command output and the URL and Stream URL fields were modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

Use this command to display information about all active MRCP sessions for the gateway. Use the **detailed** keyword to display additional information about the sessions.

Examples

The following is sample output from this command:

```
Router# show mrcp client session active

No Of Active MRCP Sessions:1

          Call-ID:0x1A
     Resource Type:Synthesizer   URL:rtsp://server-asr/synthesizer
Method In Progress:SPEAK State:SPEAKING
     Resource Type:Recognizer    URL:rtsp://server-asr/recognizer
Method In Progress:RECOGNIZE State:RECOGNIZING
```

The following is sample output when the **detailed** keyword is used:

```
Router# show mrcp client session active detailed

No Of Active MRCP Sessions: 1

           Call-ID: 0x14 same: 0
------------------------------------------
     Resource Type: Synthesizer            URL: sip:mrcpv2TTSServer@10.5.18.224
Method In Progress: SPEAK               State: S_SYNTH_IDLE

Associated CallID: 0x17
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224    Port: 51000

    Data Protocol: RTP Server IP Address: 10.5.18.224    Port: 10000
```

```
Stream URL: sip:mrcpv2TTSServer@10.5.18.224:5060

Packets Transmitted: 0 (0 bytes)
Packets Received: 177 (28320 bytes)
ReceiveDelay: 100     LostPackets: 0
-------------------------------------------
-------------------------------------------
     Resource Type: Recognizer              URL: sip:mrcpv2ASRServer@10.5.18.224
Method In Progress: RECOGNITION-START-TIMERS             State: S_RECOG_RECOGNIZING

Associated CallID: 0x18
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224     Port: 51001

    Data Protocol: RTP Server IP Address: 10.5.18.224     Port: 10002

Packets Transmitted: 191 (30560 bytes)
Packets Received: 0 (0 bytes)
ReceiveDelay: 100     LostPackets: 0
```

Table 136 describes the fields shown in this output.

Table 136 show mrcp client session active detailed Field Descriptions

Field	Description
No. Of Active MRCP Sessions	Number of MRCP sessions that are currently active between the gateway and the media server.
Call-ID	Unique identification number for the call, in hexadecimal.
Resource Type	Whether the media server being used is a speech synthesizer (TTS) or a speech recognizer (ASR).
URL	URL of the media server.
Method In Progress	Type of event that was initiated between the gateway and the media server. Values are defined by the MRCP informational RFC. For speech synthesis, values are IDLE, SPEAK, SET-PARAMS, GET-PARAMS, STOP, or BARGE-IN-OCCURRED. For speech recognition, values are DEFINE-GRAMMAR, RECOGNIZE, SET-PARAMS, GET-PARAMS, STOP, GET-RESULT, or RECOGNITION-START-TIMERS.
State	Current state of the method in progress. Values are defined by the MRCP informational RFC. For speech synthesis, values are SYNTH_IDLE, SPEAKING, SYNTH_ASSOCIATING, PAUSED, or SYNTH_ERROR_STATE. For speech recognition, values are RECOG_IDLE, RECOG_ASSOCIATING, RECOGNIZING, RECOGNIZED, or RECOG_ERROR_STATE.
Associated CallID	Unique identification number for the associated MRCP session, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.
Data Protocol	Data protocol being used, which is always RTP.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.

Table 136 show mrcp client session active detailed Field Descriptions (continued)

Field	Description
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.
show mrcp client statistics hostname	Displays statistics about MRCP sessions.

show mrcp client session history

To display information about past Media Resource Control Protocol (MRCP) client sessions that are stored on the gateway, use the **show mrcp client session history** command in privileged EXEC mode.

show mrcp client session history [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each MRCP session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version field was added to the command output and the URL field was modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

The maximum number of inactive MRCP sessions that are stored in history is configured by using the **mrcp client session history records** command. If the **mrcp client session history records** command is not used, the maximum number of history records that are saved is 50.

MRCP history records are stored for the length of time that is specified by the **mrcp client session history duration** command. If the **mrcp client session history duration** command is not configured, MRCP history records are stored for a maximum of 3600 seconds (1 hour).

Examples

The following is sample output from this command:

```
Router# show mrcp client session history

MRCP Session ID:0x9
Associated CallID:0x1A
Control Protocol:TCP     Data Protocol:RTP

Local  IP Address:10.1.2.230     Local  Port 17120
Server IP Address:10.1.2.58     Server Port 4858
Stream URL:rtsp://server-asr:554

Packets Transmitted:423 (101520 bytes)
Packets Received:819 (131040 bytes)

MRCP Session ID:0x8
Associated CallID:0x16
Control Protocol:TCP     Data Protocol:RTP

Local  IP Address:10.1.2.230     Local  Port 16948
Server IP Address:10.1.2.58     Server Port 4850
Stream URL:rtsp://server-asr:554
```

```
Packets Transmitted:284 (68160 bytes)
Packets Received:598 (95680 bytes)

MRCP Session ID:0x7
Associated CallID:0x12
Control Protocol:TCP     Data Protocol:RTP

Local  IP Address:10.1.2.230     Local  Port 16686
Server IP Address:10.1.2.58     Server Port 4842
Stream URL:rtsp://server-asr:554

Packets Transmitted:353 (84720 bytes)
Packets Received:716 (114560 bytes)

MRCP Session ID:0x6
Associated CallID:0xE
Control Protocol:TCP     Data Protocol:RTP

Local  IP Address:10.1.2.230     Local  Port 19398
Server IP Address:10.1.2.58     Server Port 4834
Stream URL:rtsp://server-asr:554

Packets Transmitted:358 (85920 bytes)
Packets Received:720 (115200 bytes)
```

The following is sample output from the **show mrcp client session history detailed** command:

```
Router# show mrcp client session history detailed

MRCP Session ID: 0x7
Associated CallID: 0x14
     MRCP version: 2.0
     =================
     Control Protocol: TCP    Data Protocol: RTP

     ASR (Callid = 0x18)
Server IP Address: 10.5.18.224     Server Port 10002
Signalling URL: sip:mrcpv2ASRServer@10.5.18.224:5060

Packets Transmitted: 373 (59680 bytes)
Packets Received: 0 (0 bytes)
OntimeRcvPlayout: 3000

GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
----------------------------------------

     TTS (Callid = 0x17)
Server IP Address: 10.5.18.224     Server Port 10000
Signalling URL: sip:mrcpv2TTSServer@10.5.18.224:5060

Packets Transmitted: 0 (0 bytes)
Packets Received: 679 (108640 bytes)
OntimeRcvPlayout: 3000

GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
```

```
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
```

Table 137 describes the fields shown in this output.

Table 137 show mrcp client session history detailed Field Descriptions

Field	Description
MRCP Session ID	Unique identification number for the MRCP session, in hexadecimal.
Associated CallID	Unique identification number for the associated call, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.
Data Protocol	Data protocol being used, which is always RTP.
ASR (Callid =)	For MRCP v2 sessions, the unique identification number for the ASR SIP call leg, in hexadecimal.
TTS (Callid =)	For MRCP v2 sessions, the unique identification number for the TTS SIP call leg, in hexadecimal.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
OntimeRcvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRcvPlayout value to the GapFill values.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GapFillWithPrediction	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding in time because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser or frame-concealment strategies in G.729 and G.723.1 compression algorithms.

Table 137 show mrcp client session history detailed Field Descriptions (continued)

Field	Description
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
HighWaterPlayoutDelay	High-water mark voice playout FIFO delay during this call.
LoWaterPlayoutDelay	Low-water mark voice playout FIFO delay during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client session history duration	Sets the maximum number of seconds for which MRCP history records are stored on the gateway
mrcp client session history records	Sets the maximum number of MRCP history records that the gateway can store.
show mrcp client session active	Displays information about active MRCP client sessions.

show mrcp client statistics hostname

To display statistics about Media Resource Control Protocol (MRCP) sessions for a specific MRCP client host, use the **show mrcp client statistics hostname** command in privileged EXEC mode.

show mrcp client statistics hostname {*hostname* | *ip-address*}

Syntax Description

hostname	Hostname of the MRCP server. Format uses host name only or hostname:port.
ip-address	IP address of the MRCP server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to display statistics about MRCP version 2 (MRCP v2) sessions.

Usage Guidelines

To display output from this command, you must first use the **mrcp client statistics enable** command.

Examples

The following is sample output from this command:

```
Router# show mrcp client statistics hostname asr-host

hostname:asr-host
Method                    :Count   Min   Avg   Max
RECOGNIZE                 :3       40    562   1604
DEFINE-GRAMMAR            :3       48    568   1604
RECOGNITION-START-TIMERS  :2       140   164   188
SPEAK                     :6       44    568   1596
RECOG-TIME                :3       804   965   1128
SPEAK-TIME                :6       3636  7063  12068
```

Table 138 describes the fields shown in this output.

Table 138 show mrcp client statistics hostname Field Descriptions

Field	Description
hostname	Host name of the media server.
Method	Type of event that was initiated between the gateway and the media server. Values as defined by the MRCP informational RFC are RECOGNIZE, DEFINE-GRAMMAR, RECOGNITION-START-TIMERS, and SPEAK. RECOG-TIME is the milliseconds that it takes the ASR server to recognize the grammar. SPEAK-TIME is the milliseconds that it takes the TTS server to speak.
Count	Total number of MRCP sessions that used this method.
Min	Length of the shortest session, in milliseconds.
Avg	Average length of a session, in milliseconds, based on all sessions.
Max	Length of the longest session, in milliseconds.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client statistics enable	Enables MRCP client statistics to be displayed.
show mrcp client session active	Displays information about active MRCP client sessions.
show mrcp client session history	Displays information about MRCP client history records that are stored on the gateway.

show mwi relay clients

To display registration information for the list of message-waiting indicator (MWI) relay clients, use the **show mwi relay clients** command in EXEC mode.

show mwi relay clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600, Cisco 3600, and Cisco IAD2420.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725 and Cisco 3745.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Examples

The following is sample output from this command:

```
Router# show mwi relay clients

Client              IPADDR       EXPIRES(sec)  MWI
============  ===============  ============   ====
4085558653       10.8.17.25       89077        ON
6505556543       10.8.17.34       87654       OFF
```

Table 139 describes significant fields shown in this output.

Table 139 show mwi relay clients Field Descriptions

Field	Description
Client	Client number.
IPADDR	IP address.
EXPIRES	Seconds before expiration.
MWI	MWI status.

Related Commands

Command	Description
mwi relay	Enables the Cisco IOS Telephony Service router to relay MWI information to remote Cisco IP phones.

show nextport

To display statistical information on NextPort digital signal processor (DSP) resources for diagnostic and debugging purposes, use the **show nextport** command in privileged EXEC mode.

show nextport {**dfc** *slot/port* | **est** [*slot/dfc/module* | **enabled**] | **ifd** {**queue** *slot/port* [**control** | **data** | **est** | **gdb** | **voice** | *npaddress* [*qid*]] | **statistics**} | **md** *modem* | **mm** [*slot/dfc/module* | **interrupt**] | **np-address** *slot/port* | **session** {*slot/port* | **tty** *ttynumber*} | **siglib test** | **ssm** {**info** *slot/port* | **test** | **vdev** *slot/port* } | **test** | **vpd** {**statistics** [*slot/port*] | **traffic** *slot/port*} | **vsmgr protocol violations**}

Syntax Description

dfc *slot/port*	Displays dial feature card (DFC) manager statistics for the specified slot and port. Range for the slot and port numbers is 1 to 7. The slash is required in the command syntax.
est	Displays Error/Status/Trace (EST) statistics for all the NextPort modules.
est *slot/dfc/module*	Displays EST information for the NextPort module in the specified slot, DFC, and module location. The slash is required in the command syntax.
est enabled	Displays a list of the enabled NextPort modules.
ifd queue *slot/port*	Displays the contents of one or more NextPort interface driver queues for the specified slot and port. Information includes the contents of the free, ready, and index rings, and the buffer description tables. The slash is required in the command syntax.
control	(Optional) Displays statistics for the interface control driver queue.
data	(Optional) Displays statistics for the interface data driver queue.
est	(Optional) Displays statistics for the interface EST driver queue.
gdb	(Optional) Displays statistics for the interface GDB driver queue.
voice	(Optional) Displays statistics for the interface voice driver queue.
npaddress	(Optional) The module address, expressed as a number (for example, 0x06000100).
qid	(Optional) Specific queue ID number. Range is from 0 to 31.
ifd statistics	Displays interface driver statistics, including any weak assertions generated.
md *modem*	Displays information for the specified NextPort modem instance.
mm	Displays modem manager information for the enabled NextPort modules.
mm *slot/dfc/module*	Displays modem manager information for the specified slot, DFC, and module location. The slash is required in the command syntax.
mm interrupt	Displays a list of system timer interrupt enabled modules.
np-address *slot/port*	Displays the NextPort address for the specified slot and port. The slash is required in the command syntax.
session *slot/port*	Displays NextPort session information for the specified slot and port. The slash is required in the command syntax.
session tty *ttynumber*	Displays NextPort session information for the specified tty session. Range is from 0 to 2003.
siglib test	Displays statistics for the SigLib test configuration.
ssm info *slot/port*	Displays information about the NextPort session and service manager (SSM) for the specified slot and port. The slash is required in the command syntax.

ssm test	Displays svc_id type, service type, and signaling type for the unit test configuration.
ssm vdev *slot/port*	Displays NextPort SSM Vdev information for the specified slot and port. The slash is required in the command syntax.
test	Displays information about the NextPort test parameters configuration.
vpd statistics *slot/port*	Displays the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics). The *slot/port* argument limits the output to statistics for the specified slot and port. The slash is required in the command syntax.
vpd traffic *slot/port*	Displays TX/RX VPD traffic statistics for the specified slot and port. The slash is required in the command syntax.
vsmgr protocol violations	Displays the number of payload violations for the NextPort voice resource manager.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	Router output for the **show nextport mm** command updated.
12.1(1)XD1	The **show nextport ifd queue** command was introduced.
12.3(11)T	This command was modified. Keywords and arguments were added to expand the variations of command output. The command was renamed **show nextport** with the **ifd queue** keyword was added.

Usage Guidelines

The **show nextport** command is intended to be used by Cisco Technical Support personnel to look at the NextPort DSP statistics and to perform detailed debugging. Please consult Cisco Technical Support before using this command.

The **show nextport** command is supported on the Cisco AS5300XM series, Cisco AS5400XM series, and Cisco AS5800XM series platforms.

When you enter the **show nextport vpd statistics** command on the Cisco AS5850, the output shows the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding. These packets are routed back to the enhanced route switch controller (ERSC).

The **show nextport vpd statistics** *slot/port* command (on individual feature boards) displays the TX/RX packet counts for the packets that have been forwarded by distributed Cisco Express Forwarding.

The display of packet counts for the packets forwarded on the Cisco AS5850 is the result of the distributed architecture of the platform.

Examples

The following examples show some of the variations of the **show nextport** command.

Note Field descriptions in the examples provided are self-explanatory.

```
Router# show nextport session 1/1

 Session Information Display
  slot/port : 1/1 TTY# : 217 Session ID : 0x006D
  Module Address : Slot 1 DFC 0 Module 0 SPE 0 Channel 1
  Service Type   : DATA FAX MODEM
  Session State  : IDLE
  TDM Information:
   DSP is connected to TDM stream 0, channel 1 on the NextPort module

Router# show nextport vpd statistics

Voice Statistics for slot 1
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 2
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 3
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 4
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
```

```
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 5
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 6
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 7
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0

Router# show nextport ssm vdev 3/1

vdev_common handle @ 0xC0D92E20

 slot 3, port 1, tone , device_status(0): VDEV_STATUS_UNLOCKED
csm_state(0x0100)=CSM_IDLE_STATE, csm_event_proc=0x601EA0C0
invalid_event_count=2, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_ISDN_STREAM(s0, u0, c0), tdm_chnl=TDM_DSP_STREAM(s3, c1)
```

```
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0x0000, bchan_num=-1
csm_event=CSM_EVENT_MODEM_ONHOOK, cause=0x0007
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=0
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0, cas_address_signalling_failure=0
call_duration_started=00:00:00, call_duration_ended=00:00:00, total_call_durati0
The calling party phone number =
The called party phone number  =
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_rtr_busy_rbs_ti,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 0, total_auto_busy_isdn_channels = 0,
total_rtr_busy_isdn_channels = 0,
min_free_device_threshold = 0

Router# show nextport mm

IOS bundled NextPort image version: 0.0.0.0
NP Module(3 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(4 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(5 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(6 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(7 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(8 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(9 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(10): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(11): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 7.37.10.90
NP Module(12): slot=4, dfc=0, module=0
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(13): slot=4, dfc=0, module=1
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(14): slot=4, dfc=0, module=2
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(15): slot=5, dfc=0, module=0
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
```

```
IOS bundled NextPort image version: 7.37.10.90
NP Module(16): slot=5, dfc=0, module=1
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(17): slot=5, dfc=0, module=2
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 0.0.0.0
NP Module(18): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(19): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(20): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(21): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(22): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(23): state = MODULE NOT INSERTED
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels.

show nextport vpd

To display the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics), use the **show nextport vpd** command in privileged EXEC mode.

show nextport vpd {**statistics** [*slot/port-number*]| **traffic** [*slot/port-number*]}

Syntax Description

statistics	Displays information about the VPD statistics.
slot/port number	(Optional) The slot or port number of the interface.
traffic	Displays TX/RX VPD traffic statistics for the specified slot and port.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show nextport vpd statistics** command displays the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding (dCEF). These packets are routed back to the enhanced route switch controller (ERSC). Executing show nextport vpd statistics slot/port (on individual feature boards) shows the TX/RX packet counts for the packets that have been forwarded by dCEF.

Examples

The following is sample output from the **show nextport vpd traffic** command for slot1 ans port1:

```
Router# show nextport vpd traffic 1/1

Voice Instance for slot 1 port 1
Status: Idle
Session Duration in second: 0
Rx traffic Statistics
  total rx bytes: 0
  total rx packets: 0
  average rx packets per second: 0
Tx traffic Statistics
  total tx bytes: 0
  total tx packets: 0
  average tx packets per second: 0
```

Table 140 describes the significant fields shown in the display.

Table 140 show nextport vpd Field Descriptions

Field	Description
Status	Current status of the voice traffic.
Session	Duration of the voice sessions in seconds.

Table 140 show nextport vpd Field Descriptions (continued)

Field	Description
Rx traffic Statistics	Number of packets received.
Tx traffic Statistics	Number of packets sent.

The following is sample output from the **show nextport vpd statistics** command. The field descriptions are self-explanatory.

```
Router# show nextport vpd statistics

Voice Instance for slot 1 port 1
Status: Idle
Rx Statistics
  rx_successful= 0
  rx_failed= 0
    queue destroyed = 0
    buffer pool depleted = 0
    invalid packet = 0
    wrong session packet = 0
Tx Statistics
  tx_successful= 0
  tx_acked_by_ifd= 0
  tx_failed= 0
    rejection by IFD = 0
```

show num-exp

To display the number expansions configured, use the **show num-exp** command in privileged EXEC mode.

show num-exp [*dialed-number*]

Syntax Description

dialed-number	(Optional) Dialed number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(4)XL	This command was implemented on the Cisco AS5800.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to display all the number expansions configured for this router. To display number expansion for only one number, specify that number by using the *dialed-number* argument.

Examples

The following is sample output from this command:

```
Router# show num-exp

Dest Digit Pattern = '0...'     Translation = '+14085270...'
Dest Digit Pattern = '1...'     Translation = '+14085271...'
Dest Digit Pattern = '3..'      Translation = '+140852703..'
Dest Digit Pattern = '4..'      Translation = '+140852804..'
Dest Digit Pattern = '5..'      Translation = '+140852805..'
Dest Digit Pattern = '6....'    Translation = '+1408526....'
Dest Digit Pattern = '7....'    Translation = '+1408527....'
Dest Digit Pattern = '8...'     Translation = '+14085288...'
```

Table 141 describes significant fields shown in this output.

Table 141 show num-exp Field Descriptions

Field	Description
Dest Digit Pattern	Index number identifying the destination telephone number digit pattern.
Translation	Expanded destination telephone number digit pattern.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call-history table.
show dial-peer voice	Displays configuration information for dial peers.
show voice port	Displays configuration information about a specific voice port.

show piafs status

To display the status of Personal Handyphone System (PHS) Internet Access Forum Standard (PIAFS) calls for each B channel in use on a router, use the **show piafs status** command in privileged EXEC mode.

show piafs status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Examples

The following is sample output from this command showing the status of PIAFS calls on B channel 1 on a Cisco 813 router:

```
Router# show piafs status

PIAFS STATUS INFORMATION
------------------------
Number of active calls = 1
Details of connection 1
**********************
Call Direction is: INCOMING
Call speed is: 64K
Current speed is: 64K
Call Elapsed Time: 59 seconds
The B channel assigned for this call is: B1 CHAN
Control Parameters Agreed Upon:
ARQ Control Information Transfer Protocol: Version 1
ARQ Data Transmission Protocol: Version 1
Measured RTF value: 9
PIAFS Frame Length in Bytes: 80
Maximum Frame Number: 63
Data Transmission Protocol of Peer: FIXED SPEED
Data Transmission Protocol of 800 Router: FIXED SPEED
V42 Negotiated: YES
V42 Parameters:
Direction: BOTH
No of code words: 4096
Max string length: 250
First PPP Frame Detected: YES
Piafs main FSM state: PIAFS_DATA
PIAFS Data Frames Tx Statistics:
Total No: of PIAFS Frames Confirmed: 344
Total Bytes of Application Data Transmitted:
Before Compression:  47021
After Compression: 30952
Compression Ratio in Tx direction is 1.51: 1
Total No: of PIAFS Frames Retransmitted: 32
```

```
Total Bytes of Application Data Retransmitted: 2336
Total Throughput in Tx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 859 Bytes/Second
Excluding PIAFS Dummy and Retransmitted Data Frames: 593 Bytes/Second
PIAFS Data Frames Rx Statistics:
Total No: of PIAFS Frames Received: 86
Total No: of Bad PIAFS Frames Received: 0
Total Bytes of Application Data Received:
Before Uncompression: 1459
After Uncompression: 2955
Compression Ratio in Rx direction is 2.02: 1
Total Throughput in Rx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 656 Bytes/Second
Excluding PIAFS Dummy and Retransmitted Data Frames: 126 Bytes/Second
No: of ReSynchronizations so far: 0
```

Table 142 describes significant fields shown in this output.

Table 142 show piafs status Field Descriptions

Field	Description
First PPP Frame Detected	If the output shows “YES,” the first PPP frame from the peer device has been detected by the Cisco 803, Cisco 804, or Cisco 813 router. If the output shows “NO,” the router has not received any PPP frames from the peer device.
Piafs main FSM state	Valid states for the finite state machine (FSM) are Initialization, Sync, Control, and Data.

Related Commands

Command	Description
debug piafs events	Displays debugging messages for PIAFS calls.

show pots csm

To display the current state of calls and the most recent event received by the call-switching module (CSM) on a Cisco 800 series router, use the **show pots csm** command in privileged EXEC mode.

show pots csm *port*

Syntax Description

port	Port number. Range is from 1 to 2.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Examples

The following is sample output from this command:

```
Router# show pots csm 1

POTS PORT: 1

   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
test pots dial	Dials a telephone number for the POTS port on the router by using a dial application on your workstation.
test pots disconnect	Disconnects a telephone call for the POTS port on the router.

show pots status

To display the settings of the telephone port physical characteristics and other information on the telephone interfaces of a Cisco 800 series router, use the **show pots status** command in privileged EXEC mode.

show pots status [**1** | **2**]

Syntax Description

1	(Optional) Displays the settings of telephone port 1.
2	(Optional) Displays the settings of telephone port 2.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Examples The following is sample output from this command.

```
Router# show pots status

POTS Global Configuration:
   Country: United States
   Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
   Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
   Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
   Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
   TX Gain: 6dB, RX Loss: -6dB,
   Filter Mask: 6F
   Adaptive Cntrl Mask: 0
POTS PORT: 1
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 10, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 2, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
```

```
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
       Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
       B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
       X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
       R: 01 11 01 90 01 90 01 90 01 90 01 90
      GZ: 60
     ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
POTS PORT: 2
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 20, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 3, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
       Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
       B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
       X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
       R: 01 11 01 90 01 90 01 90 01 90 01 90
      GZ: 60
     ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
Time Slot Control: 0
```

Table 143 describes significant fields shown in this output.

Table 143 show pots status Field Descriptions

Field	Descriptions
POTS Global Configuration	Settings of the telephone port physical characteristic commands. Also displays the following: • TX GAIN—Current transmit gain of telephone ports. • RX LOSS—Current transmit loss of telephone ports. • Filter Mask—Value determines which filters are currently enabled or disabled in the telephone port hardware. • Adaptive Cntrl Mask—Value determines if telephone port adaptive line impedance hardware is enabled or disabled.
Hook Switch Finite State Machine	Device driver that tracks state of telephone port hook switch.
CODEC Finite State Machine	Device driver that controls telephone port codec hardware.
CODEC Registers	Register contents of telephone port codec hardware.
CODEC Coefficients	Codec coefficients selected by telephone port driver. Selected line type determines codec coefficients.
CSM Finite State Machine	State of call-switching module (CSM) software.
Time Slot Control	Register that determines if telephone port voice or data packets are sent to an ISDN B channel.

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.

Command	Description
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.

show pots volume

To display the receiver volume level that is configured for each POTS port on a router, use the **show pots volume** command in privileged EXEC mode.

show pots volume

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Examples

The following is sample output from this command showing that the receiver volume level is 5 for both POTS port 1 and POTS port 2.

```
Router# show pots volume

POTS PORT 1: Volume 5
POTS PORT 2: Volume 5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
volume	Configures the receiver volume level for a POTS port on a router.

show presence global

To display configuration information about the presence service, use the **show presence global** command in user EXEC or privileged EXEC mode.

show presence global

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays the configuration settings for presence.

Examples

The following example displays output from the **show subscription global** command:

```
Router# show subscription global

Presence Global Configuration Information:
==========================================
Presence feature enable            : TRUE
Presence allow external watchers   : FALSE
Presence max subscription allowed  : 100
Presence number of subscriptions   : 0
Presence allow external subscribe  : FALSE
Presence call list enable          : TRUE
Presence server IP address         : 0.0.0.0
Presence sccp blfsd retry interval : 60
Presence sccp blfsd retry limit    : 10
Presence router mode               : CME mode
```

Table 144 describes the significant fields shown in the display.

Table 144 show subscription global Field Descriptions

Field	Description
Presence feature enable	Indicates whether presence is enabled on the router with the **presence** command.
Presence allow external watchers	Indicates whether internal presentities can be watched by external watchers, as set by the **watcher all** command
Presence max subscription allowed	Maximum number of presence subscriptions allowed by the **max-subscription** command.

Table 144 show subscription global Field Descriptions (continued)

Field	Description
Presence number of subscriptions	Current number of active presence subscriptions.
Presence allow external subscribe	Indicates whether internal watchers are allowed to subscribe to status notifications from external presentities, as set by the **allow subscribe** command.
Presence call list enable	Indicates whether the Busy Lamp Field (BLF) call-list feature is enabled with the **presence call-list** command.
Presence server IP address	Displays the IP address of an external presence server defined with the **server** command.
Presence sccp blfsd retry interval	Retry timeout, in seconds, for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence sccp blfsd retry limit	Maximum number of retries allowed for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence router mode	Indicates whether the configuration mode is set to Cisco Unified CME or Cisco Unified SRST by the **mode** command.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
debug presence	Displays debugging information about the presence service.
presence enable	Allows the router to accept incoming presence requests.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

show presence subscription

To display information about active presence subscriptions, use the **show presence subscription** command in user EXEC or privileged EXEC mode.

show presence subscription [**details** | **presentity** *telephone-number* | **subid** *subscription-id* | **summary**]

Syntax Description

details	(Optional) Displays detailed information about presentities, watchers, and presence subscriptions.
presentity *telephone-number*	(Optional) Displays information on the presentity specified by the destination telephone number.
subid *subscription-id*	(Optional) Displays information for the specific subscription ID.
summary	(Optional) Displays summary information about active subscription requests.

Command Default

Information for all active presence subscriptions is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays details about the currently active presence subscriptions

Examples

The following is sample output from the **show presence subscription details** command:

```
Presence Active Subscription Records Details:
=============================================

Subscription ID         : 1
  Watcher               : 6002@10.4.171.60
  Presentity            : 6005@10.4.171.34
  Expires               : 3600 seconds
  Subscription Duration : 1751 seconds
  line status           : idle
  watcher type          : local
  presentity type       : local
  Watcher phone type    : SIP Phone
  subscription type     : Incoming Indication
  retry limit           : 0
  sibling subID         : 0
  sdb                   : 0
```

```
  dp                    : 6555346C
  watcher dial peer tag : 40001
  number of presentity  : 1

Subscription ID         : 2
  Watcher               : 6002@10.4.171.60

Presence Active Subscription Records:
=============================================

Subscription ID         : 30
  Watcher               : 4085256003@10.4.171.34
  Presentity            : 5001@10.4.171.20
  Expires               : 3600 seconds
  line status           : idle
  watcher type          : local
  presentity type       : remote
  Watcher phone type    : SCCP [BLF Call List]
  subscription type     : Outgoing Request
  retry limit           : 0
  sibling subID         : 23
  sdb                   : 0
  dp                    : 0
  watcher dial peer tag : 0
```

The following is sample output from the **show presence subscription summary** command:

```
Router# show presence subscription summary

Presence Active Subscription Records Summary: 15 subscription
Watcher                 Presentity              SubID  Expires SibID  Status
======================= ======================= ====== ======= ====== ======
6002@10.4.171.60        6005@10.4.171.34         1     3600    0      idle
6005@10.4.171.81        6002@10.4.171.34         6     3600    0      idle
6005@10.4.171.81        6003@10.4.171.34         8     3600    0      idle
6005@10.4.171.81        6002@10.4.171.34         9     3600    0      idle
6005@10.4.171.81        6003@10.4.171.34         10    3600    0      idle
6005@10.4.171.81        6001@10.4.171.34         12    3600    0      idle
6001@10.4.171.61        6003@10.4.171.34         15    3600    0      idle
6001@10.4.171.61        6002@10.4.171.34         17    3600    0      idle
6003@10.4.171.59        6003@10.4.171.34         19    3600    0      idle
6003@10.4.171.59        6002@10.4.171.34         21    3600    0      idle
6003@10.4.171.59        5001@10.4.171.34         23    3600    24     idle
6002@10.4.171.60        6003@10.4.171.34         121   3600    0      idle
6002@10.4.171.60        5002@10.4.171.34         128   3600    129    idle
6005@10.4.171.81        1001@10.4.171.34         130   3600    131    busy
6005@10.4.171.81        7005@10.4.171.34         132   3600    133    idle
```

The following is sample output from the **show presence subscription subid** command:

```
Router# show presence subscription subid 133

Presence Active Subscription Records:
=============================================

Subscription ID         : 133
  Watcher               : 6005@10.4.171.34
  Presentity            : 7005@10.4.171.20
  Expires               : 3600 seconds
  line status           : idle
  watcher type          : local
  presentity type       : remote
  Watcher phone type    : SIP Phone
  subscription type     : Outgoing Request
```

```
retry limit           : 0
sibling subID         : 132
sdb                   : 0
dp                    : 0
watcher dial peer tag : 0
```

Table 144 describes the significant fields shown in the display.

Table 145 show presence subscription Field Descriptions

Field	Description
Watcher	IP address of the watcher.
Presentity	IP address of the presentity.
Expires	Number of seconds until the subscription expires. Default is 3600.
line status	Status of the line: • Idle—Line is not being used. • In-use—User is on the line, whether or not this line can accept a new call. • Unknown—Phone is unregistered or this line is not allowed to be watched.
watcher type	Whether the watcher is local or remote.
presentity type	Whether the presentity is local or remote.
Watcher phone type	Type of phone, either SCCP or SIP.
subscription type	The type of presence subscription, either incoming or outgoing.
retry limit	Maximum number of times the router attempts to subscribe for the line status of an external SCCP phone when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. Set with the **sccp blf-speed-dial retry-interval** command.
sibling subID	Sibling subscription ID if presentity is remote. If value is 0, presentity is local.
sdb	Voice port of the presentity.
dp	Dial peer of the presentity.
watcher dial peer tag	Dial peer tag of the watcher device.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
debug ephone blf	Displays debugging information for Busy Lamp Field (BLF) presence features.
debug presence	Displays debugging information about the presence service.
presence	Enables presence service and enters presence configuration mode.

Command	Description
presence enable	Allows the router to accept incoming presence requests.
show presence global	Displays configuration information about the presence service.

show proxy h323 calls

To display a list of active calls on the proxy, use the **show proxy h323 calls** command in privileged EXEC mode.

show proxy h323 calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from this command:

```
Router# show proxy h323 calls

Call unique key = 1
  Conference ID = [277B87C0A283D111B63E00609704D8EA]
  Calling endpoint call signalling address = 55.0.0.41
  Calling endpoint aliases:
   H323_ID: ptel11@zone1.com
  Call state = Media Streaming
  Time call was initiated = 731146290 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 detail-call	Displays the details of a particular call on a proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 detail-call

To display the details of a particular call on a proxy, use the **show proxy h323 detail-call** command in privileged EXEC mode.

show proxy h323 detail-call *call-key*

Syntax Description

call-key	Call to be displayed, derived from the **show proxy h323 calls** command output.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

You can use this command with or without proxy statistics enabled.

Examples

The following is sample output from this command without proxy statistics enabled:

```
Router# show proxy h323 detail-call 1

ConferenceID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint aliases:
      H323_ID: ptel11@zone1.com
Called endpoint aliases:
      H323_ID: ptel21@zone2.com
Peer proxy call signalling address = 172.17.0.41
Time call was initiated = 731146290 ms
Inbound CRV = 144
Outbound CRV = 70
Call state = Media Streaming
H245 logical channels for call leg pte111@zone1.com<->px1@zone.com
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
```

```
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
H245 logical channels for call leg pte111@zone1.com<->172.17.50.21:
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
```

The following is sample output from this command with proxy statistics enabled:

```
Router# show proxy h323 detail-call 1

ConferenceID = [677EB106BD0D111976200002424F832]
Calling endpoint call signalling address = 172.21.127.49
    Calling endpoint aliases:
      H323_ID: intel2
      E164_ID: 2134
Called endpoint aliases:
      H323_ID: mcs@sanjose.cisco.com
Peer proxy call signalling address = 172.68.183.199
Peer proxy aliases:
      H323_ID: proxy.sanjose.cisco.com
Time call was initiated = 730949651 ms
Inbound CRV = 2505
Outbound CRV = 67
Call state = H245 open logical channels
H245 logical channels for call leg intel2 <-> cisco7-pxy:
    Channel number = 259
      RTP stream from intel2 to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
    Channel number = 257
      RTP stream from intel2 to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
    Channel number = 2
      RTP stream from cisco7-pxy to intel2
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
        RTP Statistics:
          Packet Received Count = 3390
```

```
Packet Dropped Count = 0
Packet Out of Sequence Count = 0
Number of initial packets used for Arrival-Spacing bin setup = 200
min_arrival_spacing = 0(ms)  max_arrival_spacing = 856(ms)
Average Arrival Rate = 86(ms)
Arrival-Spacing(ms)   Packet-Count
   0                     2116
   26                    487
   52                    26
   78                    0
   104                   0
   130                   1
   156                   0
   182                   1
   208                   0
   234                   4
   260                   99
   286                   315
   312                   154
   338                   8
   364                   0
   390                   2
   416                   10
   442                   73
   468                   51
   494                   43
============================
Min Jitter = 34(ms)  Max Jitter = 408(ms)
Average Jitter Rate = 117
Jitter Rate(ms)   Packet-Count
   0                     0
   41                    514
   82                    2117
Number of initial packets used for Arrival-Spacing bin setup = 200
min_arrival_spacing = 32(ms)  max_arrival_spacing = 96(ms)
Average Arrival Rate = 60(ms)
Arrival-Spacing(ms)   Packet-Count
   32                    35
   34                    0
   36                    177
   38                    0
   40                    56
   42                     0
   44                    10
   46                    0
   48                    27
   50                    0
   52                    541
   54                    0
   56                    2642
   58                    1
   60                    1069
   62                    0
   64                    77 0
   68                    6
   70                    257
============================
Min Jitter = 0(ms)  Max Jitter = 28(ms)
Average Jitter Rate = 5
Jitter Rate(ms)   Packet-Count
   0                     1069
   3                     2720
   6                     0
   9                     804
```

```
              12                    27
              15                    10
              18                    0
              21                    56
              24                    177
              27                    35
H245 logical channels for call leg cisco7-pxy <->
proxy.sanjose.cisco.com:
    Channel number = 259
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
        RTP Statistics:
          Packet Received Count = 3398
          Packet Dropped Count = 1
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
          min_arrival_spacing = 0(ms)  max_arrival_spacing = 872(ms)
          Average Arrival Rate = 85(ms)
          Arrival-Spacing(ms)   Packet-Count
             0                     2636
             28                    0
             56                    0
             84                    0
             112                   0
             140                   1
             168                   0
             196                   0
             224                   0
             252                   0
             280                   2
             308                   425
             336                   154
             364                   5
             392                   0
             420                   0
             448                   0
             476                   114
             504                   41
             532                   20
          ==============================
          Min Jitter = 55(ms)  Max Jitter = 447(ms)
          Average Jitter Rate = 127
          Jitter Rate(ms)   Packet-Count
             0                     0
             45                    1
             90                    2636
             135                   0
             180                   2
             225                   425
             270                   159
             315                   0
             360                   0
             405                   175
    Channel number = 257
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
        RTP Statistics:
          Packet Received Count = 2537
```

```
        Packet Dropped Count = 3
        Packet Out of Sequence Count = 0
        Number of initial packets used for Arrival-Spacing bin setup = 200
        min_arrival_spacing = 0(ms)  max_arrival_spacing = 32716(ms)
        Average Arrival Rate = 112(ms)
        Arrival-Spacing(ms)   Packet-Count
           0                     2191
           72                    253
           144                   31
           216                   7
           288                   3
           360                   4
           432                   4
           504                   2
           576                   1
           648                   3
           720                   2
           792                   1
           864                   2
           936                   1
           1008                  1
           1080                  1
           1152                  1
           1224                  1
           1296                  0
           1368                  28
        ============================
        Min Jitter = 32(ms)  Max Jitter = 1256(ms)
        Average Jitter Rate = 121
        Jitter Rate(ms)   Packet-Count
           0                     284
           126                   2201
           252                   4
           378                   6
           504                   4
           630                   3
           756                   2
           882                   2
           1008                  2
           1134                  29
    Channel number = 2
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
    Channel number = 1
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949661 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
h323 qos	Enables QoS on the proxy.
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 status

To display the overall status of a proxy, use the **show proxy h323 status** command in privileged EXEC mode.

show proxy h323 status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from this command:

```
Router# show proxy h323 status

  H.323 Proxy Status
        ==================
    H.323 Proxy Mode: Enabled
    Proxy interface = Serial1: UP
    Application Specific Routing: Disabled
    RAS Initialization: Complete
    Proxy aliases configured:
      H323_ID: px2
    Proxy aliases assigned by Gatekeeper:
      H323_ID: px2
    Gatekeeper multicast discovery: Disabled
    Gatekeeper:
        Gatekeeper ID: gk.zone2.com
        IP address: 70.0.0.31
    Gatekeeper registration succeeded
    T.120 Mode: BYPASS
    RTP Statistics: OFF
    Number of calls in progress: 1
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 detail-call	Displays the details of a particular call on a proxy.

show raw

To display leaking raw buffers that have been captured, use the **show raw** command in privileged EXEC mode.

show raw {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the record of all sections.
cas	Displays the record of channel-associated signaling (CAS).
ccapi	Displays the application programming interface (API) that is used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the record of the H.323 subsystem.
ivr	Displays the record of interactive voice response (IVR).
reclaimed	Displays the raw buffers reclaimed by the audit module.
tsp	Displays the telephony service provider (TSP) subsystem.
vtsp	Displays the voice telephony service provider (VTSP) subsystem.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XU3	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The number of raw leaks that are displayed by the **show raw reclaimed** command should be zero, indicating that there are no memory leaks.

Examples

The following is a sample output from this command showing that there are no leaking raw buffers:

```
Router# show raw reclaimed

RAW LEAK REPORT:
ORPHAN    : 0       raw buffers reclaimed
TSP       : 0       raw buffers reclaimed
VTSP      : 0       raw buffers reclaimed
H323      : 0       raw buffers reclaimed
SIP       : 0       raw buffers reclaimed
CCAPI     : 0       raw buffers reclaimed
VOATM     : 0       raw buffers reclaimed
XGCP      : 0       raw buffers reclaimed
CAS       : 0       raw buffers reclaimed
IVR       : 0       raw buffers reclaimed
SSAPP     : 0       raw buffers reclaimed
Last Audit Session is at 20:28:13 UTC Fri Mar 27 2002
```

Table 146 describes significant fields shown in this output.

Table 146 show raw reclaimed Field Descriptions

Field	Description
ORPHAN	Raw buffers when a valid owner is not found.
TSP	Raw buffers on the telephony service provider (TSP) subsystem.
VTSP	Raw buffers on the voice telephony service provider (VTSP) subsystem.
H323	Raw buffers on the H.323 subsystem.
SIP	Raw buffers on the Session Initiation Protocol session.
CCAPI	Raw buffers on the API system used to coordinate interaction between application and call legs (telephony or IP).
VOATM	Raw buffers on the Voice over ATM network.
XGCP	Raw buffers on external media gateway control protocols. Includes Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
CAS	Raw buffers on the channel-associated signaling (CAS).
IVR	Raw buffers on the interactive voice response (IVR) system.
SSAPP	Raw buffers on the session application.

Related Commands

Command	Description
show rawmsg	Shows raw messages owned by the required component.

show rawmsg

To display the raw messages owned by the required component, use the **show rawmsg** command in privileged EXEC mode.

show rawmsg {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the raw messages owned by all the components.
cas	Displays the Channel Associated Signaling (CAS) subsystem.
ccapi	Displays the Application programming interface (API) used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the H.323 subsystem.
ivr	Displays the Interactive Voice Response (IVR) subsystem.
reclaimed	Displays the raw reclaimed by the audit module.
tsp	Displays the Telephony Service Provider (TSP) subsystem.
vtsp	Displays the Voice Telephony Service Provider (VTSP) subsystem.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cas**, **ivr**, and **reclaimed** keywords were added.

Usage Guidelines

The number displayed for the **show rawmsg all** command should be zero to indicate that there are no memory leaks.

Examples

The following is a sample output from the **show rawmsg tsp** command that displays memory leaks from the Telephony Service Provider. The field names are self-explanatory.

```
Router# show rawmsg tsp

 Raw Msg Summary:
       Raw Msg in used: 0
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.

show rlm group statistics

To display the network latency of a Redundant Link Manager (RLM) group, use the **show rlm group statistics** command in privileged EXEC mode.

show rlm group [*group-number*] **statistics**

Syntax Description

group-number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the network latency of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group statistics** command displays the network latency of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group statistics** command:

```
Router# show rlm group statistics

RLM Group Statistics
 Link_up:
     last time occurred at 02:45:48.724, total transition=1
     avg=00:00:00.000, max=00:00:00.000, min=00:00:00.000, latest=00:00:00.000
 Link_down:
     last time occurred at 02:42:33.724, total transition=1
     avg=00:03:15.000, max=00:03:15.000, min=00:00:00.000, latest=00:03:15.000
 Link_recovered:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Link_switched:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server_changed:
     last time occurred at 00:00:00.000 for totally 0 times
 Server Link Group[r1-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:47:15.724, success=91(62%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Open the link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
```

```
  Echo over link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:47:19.724, success=95(63%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

 Server Link Group[r2-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

Open the link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

Table 147 describes the significant fields shown in the display.

Table 147 show rlm group statistics Field Descriptions

Field	Description
Link_up	Statistics collected when the RLM group is in the link up state.
total transition	Total number of transitions into a particular RLM group state.
avg	Total average time (in seconds) that the interval lasts.
max	Total maximum time (in seconds) that the interval lasts.
min	Total minimum time (in seconds) that the interval lasts.
latest	The most recent interval.
Link_down	Statistics collected when the RLM group is in the link down state.
Link_recovered	Statistics collected when the RLM group is in the link recovery state.
Link_switched	Statistics collected when the RLM group is in the link switching state.
Server_changed	Statistics collected for when and how many times an RLM server failover happens.
Server Link Group[r1-server]	Statistics collected for the signaling links defined under a particular server link group, for example, r1-server.
Open the link	Statistics collected when a particular signaling link connection is open (broken).
Echo over link	Statistics collected when a particular signaling link connection is established.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group status	Displays the status of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group status

To display the status of a Redundant Link Manager (RLM) group, use the **show rlm group status** command in privileged EXEC mode.

show rlm group [*group-number*] **status**

Syntax Description

group-number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the status of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group status** command displays the status of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group status** command:

```
Router# show rlm group status

RLM Group 1 Status
 User/Port: RLM_MGR/3000
 Link State: Up         Last Link Status Reported: Up
 Next tx TID: 1         Last rx TID: 0
 Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[active]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[standby]
 Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening]
```

Table 148 describes the significant fields shown in the display.

Table 148 show rlm group status Field Descriptions

Field	Description
User/Port	List of registered RLM users and the port numbers associated with them.
RLM_MGR	RLM management module.
Link State	Current RLM group's link state for connecting to the remote end.
Last Link Status Reported	Most recent link status change is reported to RLM users.

Table 148 show rlm group status Field Descriptions (continued)

Field	Description
Next tx TID	Next transaction ID for transmission.
Last rx TID	Most recent transaction ID has been received.
Server Link Group[r1-server]	Status of all signaling links configured under a particular RLM server link group, for example, r1-server.
socket	Status of the individual signaling link.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group timer

To display the current timer values of a Redundant Link Manager (RLM) group, use the **show rlm group timer** command in privileged EXEC mode.

show rlm group [*group-number*] **timer**

Syntax Description

group-number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the timer values of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group timer** command displays the timer values of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group timer** command:

```
Router# show rlm group timer

RLM Group 1 Timer Values
 open_wait   = 3s                force-down  = 30s
 recovery    = 12s               switch-link = 5s
 minimum-up  = 60s               retransmit  = 1s
 keepalive   = 1s
```

Table 149 describes the significant fields shown in the display.

Table 149 show rlm group timer Field Descriptions

Field	Description
open_wait	Wait for the connection request to be acknowledged.
recovery	Time (in seconds) to allow the link to recover to backup link before declaring the link is down.
minimum-up	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.
keepalive	A keepalive packet is sent out from the network access server to the Card Security Code (CSC) periodically.
force-down	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.

Table 149 show rlm group timer Field Descriptions (continued)

Field	Description
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM goes into the recovery state.
retransmit	Because RLM is operating under User Datagram Protocol (UDP), it needs to resend the control packet if the packet is not acknowledged within this retransmit interval (in seconds).

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group status	Displays the status of an RLM group.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rpms-proc counters

To display statistics for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **show rpms-proc counters** command in privileged EXEC mode.

show rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following sample output displays leg 3 statistics for AAA preauthentication requests, successes, and rejects:

```
Router# show rpms-proc counters

H323 Calls

Preauth Requests Sent      : 43433
Preauth Requests Accepted  : 43433
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0

SIP Calls

Preauth Requests Sent      : 43080
Preauth Requests Accepted  : 43080
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
```

Table 150 describes significant fields shown in this output.

Table 150 show rpms-proc counters Field Descriptions

Field	Description
Preauth Requests Sent	Number of preauthentication requests sent.
Preauth Requests Accepted	Number of preauthentication requests accepted.
Preauth Requests Rejected	Number of preauthentication requests rejected.

Table 150 show rpms-proc counters Field Descriptions (continued)

Field	Description
Preauth Requests Timed Out	Number of preauthentication requests rejected because they timed out.
Disconnects during Preauth	Number of calls that were disconnected during the preauthentication process.

Related Commands

Command	Description
clear rpms-proc counters	Clears statistics counters for AAA preauthentication requests, successes, and rejects.

show rtpspi

To display Real-time Transport Protocol (RTP) serial peripheral interface (SPI) active call details and call statistics, use the **show rtpspi** command in privileged EXEC mode.

show rtpspi {**call** | **statistics**}

Syntax Description

call	Displays RTP SPI active call details.
statistics	Displays RTP SPI call statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **show rtpspi statistics** command:

```
Router# show rtpspi statistics

RTP Statistics info:
No. CallId     Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Latenc
1   48         0x3BA     0x25440    0x17       0xD99      0x0        0x0      0x0
2   50         0x3BA     0x4A88     0x70       0x8AD      0x0        0x0      0x0
```

Table 151 describes the significant fields shown in the display.

Table 151 show rtpspi statistics Field Descriptions

Field	Description
CallId	The call ID number.
Xmit-pkts	Number of packets transmitted.
Xmit-bytes	Number of bytes transmitted.
Rcvd-pkts	Number of packets received.
Rcvd-bytes	Number of bytes received.
Lost pkts	Number of lost packets.
Jitter	Reports the jitter encountered.
Latenc	Reports the level of latency on the call.

Related Commands

Command	Description
debug rtpspi all	Debugs all RTP SPI errors, sessions, and in/out functions.

show rtsp client session

To display cumulative information about Real Time Streaming Protocol (RTSP) session records, use the **show rtsp client session** command in privileged EXEC mode.

show rtsp client session {**history** | **active**} [**detailed**]

Syntax Description

history	Displays cumulative information about the session, packet statistics, and general call information such as call ID, session ID, individual RTSP stream URLs, packet statistics, and play duration.
active	Displays session and stream information for the stream that is currently active.
detailed	(Optional) Displays session and stream information in detail for all streams that are associated with the session. This keyword is not available on Cisco 7200 series routers.

Command Default Active (current) stream information is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Usage Guidelines Use this command to display cumulative information about the session, packet statistics, and general call information such as call ID and session ID.

Note Session refers to a session between the application and the RTSP client. Each call leg that is configured to use RTSP streaming has a session.

A call leg could play several prompts in a session; the “Play Time” refers to the play time associated with a stream or, in other words, a prompt; the cumulative play time is the sum total of all streams (or prompts) played out in a session.

The command output is a stream block that contains information about the stream (URL, packet statistics, current state of the stream, play duration, call ID, session ID, individual RTSP stream URLs, and packet statistics).

Examples

The following is sample output from the **show rtsp client session active** command:

```
Router# show rtsp client session active

RTSP Session ID:0x8     Current Status:RTSP_STATUS_PLAYING
Associated CallID:0xF
Active Request:RTSP_API_REQ_PLAY
Control Protocol:TCP     Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:708 (226560 bytes)

Cumulative Elapsed Play   Time:00:00:28.296
Cumulative Elapsed Record Time:00:00:00.000

        Session ID:0x8     State:ACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

        Packets Transmitted:0 (0 bytes)
        Packets Received:708 (226560 bytes)

        Elapsed Play   Time:00:00:28.296
        Elapsed  Record Time:00:00:00.000
        ReceiveDelay:85     LostPackets:0
```

The following is sample output from the **show rtsp client session history detailed** command:

```
Router# show rtsp client session history detailed

RTSP Session ID:0x8
Associated CallID:0xF
Control Protocol:TCP     Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:2398 (767360 bytes)

Cumulative Elapsed Play   Time:00:01:35.916
Cumulative Elapsed Record Time:00:00:00.000

        Session ID:0x8     State:INACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

        Packets Transmitted:0 (0 bytes)
        Packets Received:2398 (767360 bytes)

        Play   Time:00:01:35.916
        Record Time:00:00:00.000
        OntimeRcvPlayout:93650
        GapFillWithSilence:0
        GapFillWithPrediction:70
        GapFillWithInterpolation:0
        GapFillWithRedundancy:0
        HighWaterPlayoutDelay:85
        LoWaterPlayoutDelay:64
```

```
ReceiveDelay:85      LostPackets:0
EarlyPackets:2      LatePackets:12
```

Table 152 describes significant fields shown in this output.

Table 152 show rtsp client session Field Descriptions

Field	Description
RTSP Session ID:0x8	Unique ID for the RTSP session.
Current Status:RTSP_STATUS_PLAYING	Current status: • RTSP_STATUS_SESSION_IDLE • RTSP_STATUS_SERVER_CONNECTED • RTSP_STATUS_PLAY_PAUSED • RTSP_STATUS_PLAY_COMPLETE
Associated CallID:0xF	ID of associated call.
Control Protocol:TCP	Transport protocol.
Data Protocol:RTP	Data protocol.
Total Packets Transmitted:0 (0 bytes)	Bytes sent out to the RTSP server.
Total Packets Received:708 (226560 bytes)	Bytes received from the server for playing.

Related Commands

Command	Description
rtsp client session history duration	Specifies the length of time for which the RTSP is kept during the session.
rtsp client session history records	Specifies the number of RTSP client session history records during the session.

show rudpv0 failures

To display SS7 Reliable User Datagram Protocol (RUDP) failure statistics, use the **show rudpv0 failures** command in privileged EXEC mode.

show rudpv0 failures

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command showing displaying RUDP failures.

```
Router# show rudpv0 failures

**** RUDP Failure Stats ****

CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventsFailure        0

NotReadyFailures           0
OptionNotSupportedFailures 0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0

EmptyBufferSendFailures    0
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0

GetDataBufFailures         0
GetBufHdrFailures          0

SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendNullFailures           0
```

```
TimerNullFailures           0
FailedRetransmits           0
IncomingPktsDropped         0
UnknownRudpEvents           0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 failures** command to 0.
show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth.

show rudpv0 statistics

To display SS7 Reliable User Datagram Protocol (RUDP) internal statistics, use the **show rudpv0 statistics** command in privileged EXEC command.

show rudpv0 statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv0 statistics** command was used.

Examples

The following is sample output from this command displaying RUDP statistics and states for two connections. The fields are self-explanatory.

```
Router# show rudpv0 statistics

*** RUDP Internal Stats ****

Connection ID: 811641AC,   Current State: OPEN

RcvdInSeq                  1
RcvdOutOfSeq               0

SoftResets                 0
SoftResetsRcvd             0

TotalPacketsSent           4828
TotalPacketsReceived       4826
TotalDataBytesSent         0
TotalDataBytesReceived     4
TotalDataPacketsSent       0
TotalDataPacketsReceived   1
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Connection ID: 81163FD4,   Current State: OPEN

RcvdInSeq                  2265
RcvdOutOfSeq               0
```

```
SoftResets                0
SoftResetsRcvd            0

TotalPacketsSent          7863
TotalPacketsReceived      6755
TotalDataBytesSent        173690
TotalDataBytesReceived    56121
TotalDataPacketsSent      2695
TotalDataPacketsReceived  2265
TotalPacketsRetrans       0
TotalPacketsDiscarded     0

Cumulative RudpV0 Statistics

RcvdInSeq                 2266
RcvdOutOfSeq              0

SoftResets                0
SoftResetsRcvd            0

TotalPacketsSent          12691
TotalPacketsReceived      11581
TotalDataBytesSent        173690
TotalDataBytesReceived    56125
TotalDataPacketsSent      2695
TotalDataPacketsReceived  2266
TotalPacketsRetrans       0
TotalPacketsDiscarded     0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 statistics** command to 0.
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 {**failures** | **parameters** | **statistics**}

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv1 statistics** command was used.

Examples

The following is sample output from this command:

```
Router# show rudpv1 failures

**** RUDPV1 Failure Stats ****

CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventQueueFailure    0
OsSpecificInitFailure      0

NotReadyFailures           0
OptionNotSupportedFailures 0
InvalidOptionFailures      0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0
```

```
GetConnRecFailures          0
FindConnRecFailures         0
EmptyBufferSendFailures     0
BufferTooLargeFailures      0
ConnNotOpenFailures         0
SendWindowFullFailures      0
GetBufHdrSendFailures       0

SendInProgressFailures      0

GetDataBufFailures          0
GetBufHdrFailures           0

SendFailures                0
SendEackFailures            0
SendAckFailures             0
SendSynFailures             0
SendRstFailures             0
SendTcsFailures             0
SendNullFailures            0

TimerFailures               0
ApplQueueFailures           0
FailedRetransmits           0
IncomingPktsDropped         0
CksumErrors                 0
UnknownRudpv1Events         0
InvalidVersion              0
InvalidNegotiation          0
```

The following is sample output from the **show rudpv1 parameters** command:

```
Router# show rudpv1 parameters

*** RUDPV1 Connection Parameters ***

Next Connection Id:61F72B6C,  Remote conn id 126000

  Conn State             OPEN
  Conn Type              ACTIVE
  Accept Negot params?   Yes
  Receive Window         32
  Send Window            32
  Receive Seg Size       384
  Send Seg Size          384

                     Requested     Negotiated
  Max Auto Reset         5             5
  Max Cum Ack            3             3
  Max Retrans            2             2
  Max OutOfSeq           3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr

Next Connection Id:61F72DAC,  Remote conn id 126218

  Conn State             OPEN
  Conn Type              ACTIVE
  Accept Negot params?   Yes
  Receive Window         32
```

```
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384

                     Requested     Negotiated
  Max Auto Reset          5             5
  Max Cum Ack             3             3
  Max Retrans             2             2
  Max OutOfSeq            3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
```

The following is sample output from **the show rudpv1 statistics** command:

```
Router# show rudpv1 statistics

*** RUDPV1 Internal Stats ****

Connection ID:61F72B6C,   Current State:OPEN

RcvdInSeq                  647
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           1011
TotalPacketsReceived       958
TotalDataBytesSent         17808
TotalDataBytesReceived     17808
TotalDataPacketsSent       742
TotalDataPacketsReceived   742
TotalPacketsRetrans        117
TotalPacketsDiscarded      38

Connection ID:61F72DAC,   Current State:OPEN

RcvdInSeq                  0
RcvdOutOfSeq               0

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           75
TotalPacketsReceived       75
TotalDataBytesSent         0
TotalDataBytesReceived     0
TotalDataPacketsSent       0
TotalDataPacketsReceived   0
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Cumulative RudpV1 Statistics

NumCurConnections          2

RcvdInSeq                  652
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0
```

```
TotalPacketsSent            1102
TotalPacketsReceived        1047
TotalDataBytesSent          18048
TotalDataBytesReceived      18048
TotalDataPacketsSent        752
TotalDataPacketsReceived    752
TotalPacketsRetrans         122
TotalPacketsDiscarded       38
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears the RUDP statistics counters.
debug rudpv1	Displays debugging information for RUDP.

show sccp

To display Skinny Client Control Protocol (SCCP) information such as administrative and operational status, use the **show sccp** command in user EXEC or privileged EXEC mode.

show sccp [**all** | **ccm group** [*number*] | **connections** [**details** | **internal** | **rsvp** | **summary**] | **server** | **statistics** | **call-identifications** | **call-references**]

Syntax Description

all	(Optional) Specifies all Skinny Client Control Protocol (SCCP) global information.
ccm	(Optional) Displays SCCP Cisco Unified Communications Manager (CUCM) group related information.
group	(Optional) Displays CUCM groups.
number	(Optional) CUCM group number that needs to be displayed.
connections	(Optional) Specifies information about the connections controlled by the SCCP transcoding and conferencing applications.
details	(Optional) Displays SCCP connections in detail.
internal	(Optional) Displays information about SCCP internal connections.
rsvp	(Optional) Displays Resource Reservation Protocol (RSVP) information about SCCP connections.
summary	(Optional) Displays information about SCCP connections.
server	(Optional) Displays SCCP server information.
statistics	(Optional) Specifies statistical information for SCCP transcoding and conferencing applications.
call-identifications	(Optional) Displays the following identification numbers that is associated with each leg of a call: • Session • Call Reference • Connection • Call • Bridge • Profile
call-references	(Optional) Displays codec, port, ID numbers for each leg of a call.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(6)T	This command was modified. The **rsvp** keyword was added.

Release	Modification
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.3(8)T	This command was modified. The following keywords and arguments were added: **ccm**, **connections**, **details**, **group**, **internal,** *number,* **summary**.
12.4(11)XW1	This command was modified. The stype field was added to the show output to show whether a connections is encrypted.
12.4(15)XY	This command was modified. The **statistics** and **server** keywords were added.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information and it was integrated into Cisco IOS Release 12.2(13)T.
15.1(4)M	This command was modified. The **call-identifications** and **call-references** keywords were added.

Usage Guidelines

The router on which you use the **show sccp** command must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use the **show sccp ccm** group command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional group-number argument can be added to select details about a specific group.

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the clear sccp server statistics command.

Examples

In the following sample output, the gateway IP address can be an IPv4 or IPv6 address when it operates on an IPv4/IPv6 dual stack.

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/0
        IPv6 Address: 2001:DB8:C18:1::3
        IPv4 Address: 10.4.34.100
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.19.242.27, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 4
                Trustpoint: N/A
Call Manager: 2001:DB8:C18:1::100, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
```

Table 153 describes the significant fields shown in the display.

Table 153 show sccp Field Descriptions

Field	Description
SCCP Admin State	Current state of the SCCP session.
Gateway Local Interface	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
IP precedence	Sets the IP precedence value for SCCP.
User Masked Codec list	Codec to mask.
Call Manager	Cisco Unified CallManager server information.

The following is sample output from this command for IPv4 only. The field descriptions are self-explanatory.

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.10.10.11, Port Number: 0
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 100
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active CallManager: 10.10.10.35, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: DOWN - Cause Code: DSPFARM_DOWN
Active CallManager: NONE
TCP Link Status: NOT_CONNECTED
CallManager: 10.10.10.37, Port Number: 2000
Priority: 3, Version: 3.1
CallManager: 10.10.10.35, Port Number: 2000
Priority: 2, Version: 3.0
```

The following sample shows statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp statistics

SCCP Transcoding Application Statistics:
TCP packets rx 548, tx 559
Unsupported pkts rx 3, Unrecognized pkts rx 0
Register tx 3, successful 3, rejected 0, failed 0
KeepAlive tx 543, successful 540, failed 2
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 1, Switchback 1

SCCP Conferencing Application Statistics:
TCP packets rx 0, tx 0
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 0, successful 0, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
```

```
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

In the following example, the secure value of the stype field indicates that the conection is encrypted. The field descriptions are self-explanatory.

```
Router# show sccp connections

sess_id    conn_id    stype        mode codec   ripaddr       rport sport

16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464

Total number of active session(s) 1, and connection(s) 2
```

The following example shows the remote IP addresses of active RTP sessions, each of which shows either an IPv4 or an IPv6 address.

```
Router# show sccp connections

sess_id  conn_id  stype  mode    codec sport rport ripaddr

16777219 16777245 conf  sendrecv g711u 16516 27814 10.3.43.46
16777219 16777242 conf  sendrecv g711u 17712 18028 10.3.43.2
16777219 16777232 conf  sendrecv g711u 16890 19440 10.3.43.2
16777219 16777228 conf  sendrecv g711u 19452 17464 10.3.43.2
16777220 16777229 xcode sendrecv g711u 17464 19452 10.3.43.2
16777220 16777227 xcode sendrecv g729b 19466 19434 2001:0DB8:C18:1:212:79FF:FED7:B254
16777221 16777233 mtp   sendrecv g711u 19440 16890 10.3.43.2
16777221 16777231 mtp   sendrecv g711u 17698 17426 2001:0DB8:C18:1:212:79FF:FED7:B254
16777223 16777243 mtp   sendrecv g711u 18028 17712 10.3.43.2
16777223 16777241 mtp   sendrecv g711u 16588 19446 2001:0DB8:C18:1:212:79FF:FED7:B254
```

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group

CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default

CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

Table 154 describes the significant fields shown in the display.

Table 154 show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Current state of the SCCP session.
Description	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Binded Interface	Sets the IP precedence value for SCCP.
Registration Retries	Codec to mask.
Registration Timeout	Cisco Unified CallManager server information.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Retries	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
CCM Connect Interval	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchover Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

The following sample output displays the summary information for all SCCP call references:

```
Router# show sccp call-reference
session_id: 16805277   session_type: vcf   , profile_id: 101,
    call-reference: 25666614   , Name: , Number: 3004
        Audio conn_id: 16777929   , str_passthr: 0
              rtp-call-id: 21         , bridge-id: 15         , msp-call-id: 12
              mode: sendrecv, sport: 25146, rport 16648, ripaddr: 10.22.82.205
              codec: g711u   , pkt-period: 20
    call-reference: 25666611   , Name: , Number: 6628
        Audio conn_id: 16777926   , str_passthr: 0
              rtp-call-id: 19         , bridge-id: 13         , msp-call-id: 12
              mode: sendrecv, sport: 28168, rport 2398 , ripaddr: 128.107.147.125
              codec: g711u   , pkt-period: 20
        Video conn_id: 16777927   , conn_id_tx: 16777928   , str_passthr: 0
```

```
              rtp-call-id: 20        , bridge-id: 14        , msp-call-id: 12
              mode: sendrecv, sport: 22604, rport 2400 , ripaddr: 128.107.147.125
              bit rate: 1100kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.2, max mbps: 81 (x500 MB/s), max fs: 7
(x256 MBs)
    call-reference: 25666608  , Name: , Number: 62783365
        Audio conn_id: 16777923  , str_passthr: 0
              rtp-call-id: 16        , bridge-id: 11        , msp-call-id: 12
              mode: sendrecv, sport: 21490, rport 20590, ripaddr: 10.22.83.142
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777924  , conn_id_tx: 16777925  , str_passthr: 0
              rtp-call-id: 17        , bridge-id: 12        , msp-call-id: 12
              mode: sendrecv, sport: 23868, rport 29010, ripaddr: 10.22.83.142
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 3.0, max mbps: 0 (x500 MB/s), max fs: 0
(x256 MBs)
    call-reference: 25666602  , Name: , Number: 62783363
        Audio conn_id: 16777916  , str_passthr: 0
              rtp-call-id: 11        , bridge-id: 7         , msp-call-id: 12
              mode: sendrecv, sport: 26940, rport 20672, ripaddr: 10.22.82.48
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777917  , conn_id_tx: 16777919  , str_passthr: 0
              rtp-call-id: 13        , bridge-id: 8         , msp-call-id: 12
              mode: sendrecv, sport: 16462, rport 20680, ripaddr: 10.22.82.48
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.0, max mbps: 72 (x500 MB/s), max fs: 5
(x256 MBs)

Total number of active session(s) 1
   Total of number of active session(s) 1
      with total of number of call-reference(s) 4
         with total of number of audio connection(s) 4
         with total of number of video connection(s) 3
```

The following sample output displays summary information for all SCCP call identifications:

```
Router# show sccp call-identifications

sess_id   callref   conn_id   conn_id_tx spid  rtp_callid msp_callid bridge_id  codec
stype prof_id
16805277  25666614  16777929  0          0     21         12         15         g711u  vcf
101
16805277  25666611  16777926  0          0     19         12         13         g711u  vcf
101
16805277  25666611  16777927  16777928   0     20         12         14         h264   vcf
101
16805277  25666608  16777923  0          0     16         12         11         g711u  vcf
101
16805277  25666608  16777924  16777925   0     17         12         12         h264   vcf
101
16805277  25666602  16777916  0          0     11         12         7          g711u  vcf
101
16805277  25666602  16777917  16777919   0     13         12         8          h264   vcf
101

Total number of active session(s) 1
```

The following sample displays the output from **show sccp**:

```
Router# show sccp

SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 172.19.156.7
        Port Number: 2000
```

```
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.4.211.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
Call Manager: 128.107.151.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 100
                Trustpoint: N/A

V_Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 128.107.151.39, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 101
Reported Max Streams: 4, Reported Max OOS Streams: 0
Layout: default 1x1
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Supported Codec: h264: QCIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: QCIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: 4CIF, Frame Rate: 30fps, Bit Rate: 1000-1000 Kbps
TLS : ENABLED
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show dspfarm	Displays summary information about DSP resources.

show sccp ccm group

To display the groups that are configured on a specific Cisco Unified CallManager, use the **show sccp ccm group** command in privileged EXEC mode.

show sccp ccm group [*group-number*]

Syntax Description

group-number	(Optional) Number that identifies the Cisco CallManager group. Range is 1 to 65535. There is no default value.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show sccp ccm group** command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional *group-number* argument can be added to select details about a specific group.

Examples

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named “boston office” and group 988 named “atlanta office”.

```
Router# show sccp ccm group

CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default

CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

Table 155 describes significant fields shown in this output.

Table 155 show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Displays the Cisco CallManager group number.
Description	Displays the optional description of the group assigned to the group number.
Binded Interface	Displays the IP address of the selected interface is used for all calls within a given profile.
Registration Retries	Number of times that SCCP tries to register with a Cisco Unified CallManger
Registration Timeout	Length of time, in seconds, between registration messages sent from SCCP to the Cisco Unified CallManager.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the length of time, in seconds, between keepalive retries.
CCM Connect Retries	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Interval	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
Switchover Method	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco Unified CallManager server to the list of available servers.

show sccp connections details

To display Skinny Client Control Protocol (SCCP) connection details such as call-leg details, use the **show sccp connections details** command in privileged EXEC mode.

show sccp connections details

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections details

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period type      bridge-info(bid, cid)
mmbridge-info(bid, cid)

16800395  -       15       N/A    N/A      transmsp  All RTPSPI Callegs     N/A

16800395  18425889  14       g711u  20       rtpspi   (10,15)             N/A

16800395  18425905  13       g711u  20       rtpspi   (9,15)              N/A


Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections internal	Displays the internal SCCP details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections internal

To display the internal Skinny Client Control Protocol (SCCP) details such as time-stamp values, use the **show sccp connections internal** command in privileged EXEC mode.

show sccp connections internal

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections internal

Total number of active session(s) 0, and connection(s) 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections details	Displays the SCCP connection details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections rsvp

To display information about active Skinny Client Control Protocol (SCCP) connections that are using RSVP, use the **show sccp connections rsvp** command in privileged EXEC mode.

show sccp connections rsvp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections rsvp

sess_id    conn_id    rsvp_id    dir  local ip       :port  remote ip      :port
16777578   16778093   -210       SEND 192.168.21.1   :18486 192.168.20.1   :16454
16777578   16778093   -211       RECV 192.168.21.1   :18486 192.168.20.1   :16454

 Total active sessions 1, connections 2, rsvp sessions 2
```

Table 156 describes the fields shown in the display.

Table 156 show sccp connections rsvp Field Descriptions

Field	Description
sess_id	Identification number of the SCCP session.
conn_id	Identification number of the SCCP connection.
rsvp_id	Identification number of the RSVP connection.
dir	Direction of the SCCP connection.
local ip	IP address of the local endpoint.
remote ip	IP address of the remote endpoint.
port	Port number of the local or remote endpoint.
Total active sessions	Total number of active SCCP sessions.
connections	Number of active connections that are a part of the SCCP sessions.
rsvp session	Number of active connections that use RSVP.

Related Commands

Command	Description
debug sccp all	Displays debugging information for SCCP.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
rsvp	Enables RSVP support on a transcoding or MTP device.
sccp	Enables SCCP on the interface.
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified CallManager.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections summary

To display a summary of the number of sessions and connections based on the service type under the Skinny Client Control Protocol (SCCP) application, use the **show sccp connections summary** command in privileged EXEC mode.

show sccp connections summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections summary

SCCP Application Service(s) Statistics Summary:
Total Conferencing Sessions: 0, Connections: 0
Total Transcoding Sessions: 0, Connections: 0
Total MTP Sessions: 0, Connections: 0
Total SCCP Sessions: 0, Connections: 0
```

Table 157 describes significant fields shown in this output.

Table 157 show sccp connections summary Field Descriptions

Field	Description
Connections	Displays the total number of current connections associated with a given application.
Total Conferencing Sessions	Displays the number of current conferencing sessions.
Total MTP Sessions	Displays the number of current Media Termination Point (MTP) sessions.
Total SCCP Sessions	Displays the number of current SCCP sessions.
Total Transcoding Sessions	Displays the number of current transcoding sessions.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections details	Displays the SCCP connection details.
show sccp connections internal	Displays the internal SCCP details.

show sccp server statistics

To display the statistical counts on the Skinny Client Control Protocol (SCCP) server, use the **show sccp server statistics** command in privileged EXEC mode.

show sccp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.

Usage Guidelines

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the **clear sccp server statistics** command.

Examples

The following example shows the SCCP statistical counts on the server:

```
Router# show sccp server statistics

Failure type              Error count
------------------------  -----------
Send queue enqueue        2
Socket send               3
Msg discarded upon error  5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear sccp server statistics	Clears the counts displayed the **under show sccp server statistics** command.

show sdspfarm

To display the status of the configured digital signal processor (DSP) farms and transcoding streams, use the **show sdspfarm** command in privileged EXEC mode.

show sdspfarm {**units** [**name** *unit-name* | **register** | **summary** | **tag** *number* | **unregister**] | **sessions** [**active** | **callID** *number* | **states** | **statistics** | **streamID** *number* | **summary**] | **message statistics**}

Syntax Description

units	Displays the configured and registered DSP farms.
name *unit-name*	(Optional) Displays the name of the unit.
register	(Optional) Displays information about the registered units.
summary	(Optional) Displays summary information about the units.
tag *number*	(Optional) Displays tag number of the unit.
unregister	(Optional) Displays information about the unregistered units.
sessions	Displays the transcoding streams.
active	(Optional) Displays all active sessions.
callID	(Optional) Displays activities for a specific caller ID.
number	(Optional) The caller ID number displayed by the **show voip rtp connection** command.
states	(Optional) Current state of the transcoding stream.
statistics	(Optional) Displays session statistics.
streamID *number*	(Optional) Displays the transcoding stream sequence number.
summary	(Optional) Displays summary information.
message	Displays message information.
statistics	Displays statistics information about the messages.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(22)T	The following combinations of keywords and arguments were added: **name**, *unit-name*, **register**, **summary**, **tag** *number*, **unregister**, **states**, **streamID** *number*, **message statistics**.

Examples

The following example displays the configured and registered DSP farms:

```
Router# show sdspfarm units

mtp-1 Device:MTP123456782012 TCP socket:[-1]  UNREGISTERED
actual_stream:0 max_stream 0 IP:0.0.0.0  0  Unknown 0 keepalive 0

mtp-2 Device:MTP000a8aeaca80 TCP socket:[5]  REGISTERED
actual_stream:40 max_stream 40 IP:10.5.49.160  11001  MTP YOKO keepalive 12074
```

```
Supported codec:G711Ulaw
                G711Alaw
                G729
                G729a
                G729b
                G729ab

 max-mtps:2, max-streams:240, alloc-streams:40, act-streams:0
```

The following is sample output from the **show sdspfarm sessions active** command:

```
Router# show sdspfarm sessions active

Stream-ID:3 mtp:2 192.0.2.0 20174  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4

Stream-ID:4 mtp:2 192.0.2.0 17072  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
```

The following is sample output from the **show sdspfarm sessions callID** command:

```
Router# show sdspfarm sessions callID 51M

Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52, confID:5,
mtp:2^
Peer Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51,
confID:5, mtp:2^
Router-2015# show sdspfarm sessions callid 52
Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51, confID:5,
mtp:2
Peer Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52,
confID:5, mtp:2
```

The following is sample output from the **show sdspfarm sessions statistics** command:

```
Router# show sdspfarm sessions statistics

Stream-ID:1 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:1014 in-pak:0 discard:0
Stream-ID:2 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:3 mtp:2 10.5.49.160  20174  Local:2000START  MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4
 recv-pak:0 xmit-pak:0 out-pak:4780 in-pak:0 discard:0
Stream-ID:4 mtp:2 10.5.49.160  17072  Local:2000START  MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:5 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:6 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:7 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:8 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:9 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
```

```
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:10 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:11 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:12 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:13 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:14 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:15 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:16 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:17 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:18 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:19 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:20 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:21 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:22 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:23 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:24 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:25 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:26 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:27 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:28 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:29 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:30 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

```
Stream-ID:31 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:32 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:33 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:34 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:35 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:36 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:37 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:38 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:39 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:40 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

The following is sample output from the **show sdspfarm sessions summary** command:

```
Router# show sdspfarm sessions summary

max-mtps:2, max-streams:240, alloc-streams:40, act-streams:2
  ID   MTP  State      CallID confID Usage                          Codec/Duration
==== ===== ====== =========== ====== ============================== ==============
1    2     IDLE   -1          0                                    G711Ulaw64k /20ms
2    2     IDLE   -1          0                                    G711Ulaw64k /20ms
3    2     START  -1          3      MoH  (DN=3  , CH=1) FE=TRUE  G729 /20ms
4    2     START  -1          3      MoH  (DN=3  , CH=1) FE=FALSE G711Ulaw64k /20ms
5    2     IDLE   -1          0                                    G711Ulaw64k /20ms
6    2     IDLE   -1          0                                    G711Ulaw64k /20ms
7    2     IDLE   -1          0                                    G711Ulaw64k /20ms
8    2     IDLE   -1          0                                    G711Ulaw64k /20ms
9    2     IDLE   -1          0                                    G711Ulaw64k /20ms
10   2     IDLE   -1          0                                    G711Ulaw64k /20ms
11   2     IDLE   -1          0                                    G711Ulaw64k /20ms
12   2     IDLE   -1          0                                    G711Ulaw64k /20ms
13   2     IDLE   -1          0                                    G711Ulaw64k /20ms
14   2     IDLE   -1          0                                    G711Ulaw64k /20ms
15   2     IDLE   -1          0                                    G711Ulaw64k /20ms
16   2     IDLE   -1          0                                    G711Ulaw64k /20ms
17   2     IDLE   -1          0                                    G711Ulaw64k /20ms
18   2     IDLE   -1          0                                    G711Ulaw64k /20ms
19   2     IDLE   -1          0                                    G711Ulaw64k /20ms
20   2     IDLE   -1          0                                    G711Ulaw64k /20ms
21   2     IDLE   -1          0                                    G711Ulaw64k /20ms
22   2     IDLE   -1          0                                    G711Ulaw64k /20ms
23   2     IDLE   -1          0                                    G711Ulaw64k /20ms
24   2     IDLE   -1          0                                    G711Ulaw64k /20ms
25   2     IDLE   -1          0                                    G711Ulaw64k /20ms
26   2     IDLE   -1          0                                    G711Ulaw64k /20ms
```

```
27    2      IDLE    -1          0                                    G711Ulaw64k /20ms
28    2      IDLE    -1          0                                    G711Ulaw64k /20ms
29    2      IDLE    -1          0                                    G711Ulaw64k /20ms
30    2      IDLE    -1          0                                    G711Ulaw64k /20ms
31    2      IDLE    -1          0                                    G711Ulaw64k /20ms
32    2      IDLE    -1          0                                    G711Ulaw64k /20ms
33    2      IDLE    -1          0                                    G711Ulaw64k /20ms
34    2      IDLE    -1          0                                    G711Ulaw64k /20ms
35    2      IDLE    -1          0                                    G711Ulaw64k /20ms
36    2      IDLE    -1          0                                    G711Ulaw64k /20ms
37    2      IDLE    -1          0                                    G711Ulaw64k /20ms
38    2      IDLE    -1          0                                    G711Ulaw64k /20ms
39    2      IDLE    -1          0                                    G711Ulaw64k /20ms
40    2      IDLE    -1          0                                    G711Ulaw64k /20ms
```

Table 158 describes the fields shown in the **show sdspfarm** command display.

Table 158 show sdspfarm Field Descriptions

Field	Description
act-streams	Active streams that are involved in calls.
alloc-streams	Number of transcoding streams that are actually allocated to all DSP farms that are registered to Cisco CME.
callID	Caller ID that the active stream is in.
Codec	Codec in use.
confID	ConfID that is used to communicate with DSP farms.
discard	Number of packets that are discarded.
dstCall-ID	Caller ID of the destination IP call leg.
Duration or dur	Packet rates, in milliseconds.
ID	Transcoding stream sequence number in Cisco CME.
in-pak	Number of incoming packets from the source call leg.
Local	Local port for voice packets.
max-mtps	Maximum number of Message Transfer Parts (MTPs) that are allowed to register in Cisco CME.
max-streams	Maximum number of transcoding streams that are allowed in Cisco CME.
mtp or MTP	MTP sequence number where the transcoding stream is located.
out-pak	Number of outgoing packets sending to source call leg.
peer Stream-ID	Stream sequence number of the other stream paired in the same transcoding session. (Two transcoding streams make up a transcoding session).
recv-pak	Number of voice packets received from the DSP farm.
srcCall-ID	Source caller ID of the source IP call leg.
State	Current state of the transcoding stream; could be IDLE, SEIZE, START, STOP, or END.
Stream-ID	Transcoding stream sequence number in Cisco CME.

Table 158 show sdspfarm Field Descriptions (continued)

Field	Description
TCP socket	Socket number for DSP farm (similar to TCP socket for **show ephone** output).
usage	Current usage of the stream; for example, Ip-Ip (IP to IP transcoding), Moh (for MOH transcoding) and Conf (conference).
vad	Voice-activity detection (VAD) flag for the transcoding stream. It should always be 0 (False).
xmit-pak	Number of packets that are sent to the DSP farm.

Related Commands

Command	Description
sdspfarm tag	Permits a DSP farm to be to registered to Cisco CME and be associated with an SCCP client interface's MAC address.
sdspfarm transcode sessions	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to Cisco CME.

show settlement

To display the configuration for all settlement servers and see specific provider and transactions, use the **show settlement** command in privileged EXEC mode.

show settlement [*provider-number* [**transactions**]]

Syntax Description

provider-number	(Optional) Displays the attributes of a specific provider.
transactions	(Optional) Displays the transaction status of a specific provider.

Defaults

Information about all servers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command displaying information about all settlement servers that are configured:

```
Router# show settlement

Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all                 (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s)    (default)
Response Timeout = 1 (s)         (default)
Retry Delay = 2 (s)              (default)
Retry Limit = 1                  (default)
Session Timeout = 86400 (s)      (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled               (default)
Signed Token = on

Number of Connections = 0
Number of Transactions = 7
```

The following is sample output from this command displaying transaction and state information about a specific settlement server:

```
Router# show settlement 0 transactions

Transaction ID=8796304133625270342
        state=OSPC_GET_DEST_SUCCESS, index=0
        callingNumber=5710868, calledNumber=15125551212
```

Table 159 describes significant fields shown in this output. Provider attributes that are not configured are not shown.

Table 159 show settlement Field Descriptions

Field	Description
type	Settlement provider type.
address url	URL address of the provider.
encryption	SSL encryption method.
max-connections	Maximum number of concurrent connections to provider.
connection-timeout	Connection timeout with provider (in seconds).
response-timeout	Response timeout with provider (in seconds).
retry-delay	Delay time between retries (in seconds).
retry-limit	Number of retries.
session-timeout	SSL session timeout (in seconds).
customer-id	Customer ID, assigned by provider.
device-id	Device ID, assigned by provider.
roaming	Roaming enabled.
signed-token	Indicates if the settlement token is signed by the server.

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after a communication exchange is completed.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

show sgcp connection

To display all active Simple Gateway Control Protocol (SGCP) connections on a router, use the **show sgcp connection** command in EXEC mode.

show sgcp connection [**interface** *number*]

Syntax Description

interface	(Optional) Displays output for a particular DS1 interface.
number	(Optional) Interface (controller) number.

Defaults

All active SGCP connections on the host are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Examples

The following is sample output from this command displaying active connections on a router:

```
Router# show sgcp connection

Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (E)vent[SIFL] (R)esult[EA]
1. ds1-0/1@r3810-5      C=1,1,2  I=0x1  P=16492,16476  M=3  S=4  E=3,0,0,3  R=0, 0
```

The following is sample output from this command displaying the state of SGCP on a router:

```
Router# show sgcp connection

SGCP Admin State DOWN, Oper State DOWN
SGCP call-agent: 209.165.200.225 , SGCP graceful-shutdown enabled? FALSE
SGCP request timeout 40, SGCP request retries 10
```

Table 160 describes significant fields shown in this output.

Table 160 show sgcp connection Field Descriptions

Field	Description
SGCP Admin State	Administrative and operational state of the SGCP daemon.
SGCP call-agent	Address of the call agent specified with the **sgcp** command.
SGCP graceful-shutdown enabled	The state of the **sgcp graceful-shutdown** command.
SGCP request timeout	The setting for the **sgcp request timeout** command.
SGCP request retries	The setting for the **sgcp request retries** command.

Related Commands

Command	Description
show sgcp endpoint	Displays SGCP endpoint information.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp endpoint

To display Simple Gateway Control Protocol (SGCP) endpoints that are eligible for SGCP management, use the **show sgcp endpoint** command in EXEC mode.

show sgcp endpoint [**interface** *ds1* [*ds0*]]

Syntax Description

interface *ds1*	(Optional) DS1 interface for which to display SGCP endpoint information. Range is from 1 to 1000.
ds0	(Optional) DS0 interface for which to display SGCP endpoint information. Range is from 0 to 30.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines

Use this command to display SGCP endpoint information for the whole router or for a specific DS1 interface and, optionally, a specific DS0. If you enter a nonexistent combination of a DS1 and DS0, the following error message appears: “No matching connection found.”

Examples

The following is sample output from this command displaying SGCP endpoint information being set for a matching connection between DS1 interface 1 and DS0 interface 10:

```
Router# show sgcp endpoint interface 1 10
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host router.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp statistics

To display global statistics for the Simple Gateway Control Protocol (SGCP) packet count, success and failure counts, and other information, use the **show sgcp statistics** command in EXEC mode.

show sgcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.0(5)T	This command was implemented on the Cisco AS5300 only in a private release that was not generally available.

Usage Guidelines

You can filter the displayed output, as shown in the examples.

Examples

The following is sample output from this command displaying SGCP packet statistics:

```
Router# show sgcp statistics

UDP pkts rx 5, tx 13
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 1, successful 1, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 3, successful 3, failed 0
Notify tx 3, successful 3, failed 0
ACK tx 4, NACK tx 0
ACK rx 1, NACK rx 0

IP address based Call Agents statistics:
IP address 1.4.63.100, Total msg rx 5,
                   successful 5, failed 2
```

The following is sample output from this command showing how to filter output for specific information:

```
Router# show sgcp statistics | begin Failed

Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
```

```
Notify tx 0, successful 0, failed 0
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0

Router# show sgcp statistics | exclude ACK

UDP pkts rx 0, tx 0
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0

Router# show sgcp statistics | include ACK

ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host Cisco AS5300 universal access server.
show sgcp endpoint	Displays SGCP endpoint information.

show shared-line

To display information about the Session Initiation Protocol (SIP) shared lines, use the **show shared-line** command in user EXEC or privileged EXEC mode.

show shared-line {**call** | **details** | **subscription** | **summary**}

Syntax Description

call	Displays information about all active calls on shared lines.
details	Displays detailed information about each shared line.
subscription	Displays information for specific subscriptions to shared lines.
summary	Displays summary information about active subscriptions to shared lines.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following is sample output from the **show shared-line call** command:

```
Router# show shared-line call

Shared-Line active call info:

Shared-Line: '20141',  active calls: 3
Local User       Local Address               Remote User       Remote Address  CallID
==========       =====================       ===========       ==================== ====
20141            20141@10.6.0.2               20143             20143@10.10.0.1 3168

20141            20141@10.6.0.1               Barge             20143@10.10.0.1 3209

20141            20141@10.6.0.2               20141             20141@10.10.0.1 3210
```

The following is sample output from the **show shared-line details** command:

```
Router# show shared-line details

Shared-Line info details:

Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
Index        Users                  sub_id         peer_tag        Status
=====        =====                  ======         ========        ======
  1          20141@10.6.0.1             5            40001           ACTIVE
  2          20141@10.6.0.2             6            40002           ACTIVE
Free call queue size: 7,   Active call queue size: 3

Message queue size: 20,   Event queue size: 64
```

The following is sample output from the **show shared-line subscription** command:

```
Router# show shared-line subscription
```

```
Shared-Line Subscription Info:

Subscriptions to: '20141',   total subscriptions: 2
SubID        Subscriber                  Expires         Sub-Status
=====        ==========                  =======         ==========
  5          20141@10.6.0.1                 3600          NOTIFY_ACKED
  6          20141@10.6.0.2                 3600          NOTIFY_ACKED
```

The following is sample output from the **show shared-line summary** command:

```
Router# show shared-line summary

Shared-Line info summary:
Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
```

Table 161 describes the significant fields shown in the displays.

Table 161 show shared-line Field Descriptions

Field	Description
Expires	Number of seconds until the subscription expires.
Local Address	IP address of the local phone involved in the shared line call.
Local User	Extension number of the shared line.
Remote Address	IP address of the remote phone involved in the shared line call.
Remote User	Extension of the remote phone involved in the shared line call.
SubID	Subscription ID.
Subscriber	Extension number of the shared line and the IP address of the phone subscriber.
Sub-Status	Status of the subscription.
Users	IP addresses of the phones using the shared line.

Related Commands

Command	Description
debug shared-line	Displays debugging information about SIP shared lines.

show sip dhcp

To display the Session Initiation Protocol (SIP) parameters retrieved via the Dynamic Host Configuration Protocol (DHCP), use the **show sip dhcp** command in privileged EXEC mode.

show sip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

If SIP parameters are configured to be retrieved via DHCP, use the **show sip dhcp** command to display the SIP parameters retrieved.

Examples

The following is sample output from the **show sip dhcp** command:

```
Router# show sip dhcp

SIP UAC DHCP Info

SIP-DHCP interface:  GigabitEthernet0/0

SIP server address:  ipv4:9.13.2.36
Pilot number:        777777
Domain name:         dns:cisco.com
Secondary number:    222222
Secondary number:    333333
Secondary number:    444444
Secondary number:    555555
Secondary number:    666666
```

Table 162 describes the significant fields shown in the display.

Table 162 show sip dhcp Field Descriptions

Field	Description
SIP-DHCP interface	Indicates the type and number of the interface assigned to be used for SIP provisioning via DHCP.
SIP server address	Displays the address of the SIP server configured on the DHCP server and retrieved via DHCP.

Table 162 show sip dhcp Field Descriptions (continued)

Field	Description
Pilot number	Displays the pilot or contract number retrieved via DHCP and registered with the SIP server. Registration is done only for the pilot number.
Domain name	Indicates the domain name of the SIP server. The Cisco Unified Border Element will try to resolve this domain name by Domain Name System (DNS) into a routable layer 3 IP address for sending Register and Invite messages.
Secondary number	Indicates the first five secondary or additional numbers retrieved from the DHCP server. Secondary numbers are not registered with the SIP server.

Related Commands

Command	Description
debug ccsip dhcp	Displays information on SIP and DHCP interaction for debugging DHCP provisioning of SIP parameters.

show sip service

To display the status of SIP call service on a SIP gateway, use the **show sip service** command in voice configuration mode.

show sip service

Syntax Description This command has no arguments or keywords

Command Default No default behaviors or values

Command Modes Voice service configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples The following example displays output when SIP call service is enabled:

```
Router# show sip service
SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip service
SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is shut down with the **shutdown forced** command:

```
Router# show sip service
SIP service is forced shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop forced** command:

```
Router# show sip service
SIP service is forced shut
under 'voice service voip', 'sip' submode
```

Field descriptions should be self-explanatory.

show sip-ua calls

To display active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls, use the **show sip-ua calls** command in privileged EXEC mode.

show sip-ua calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(22)T	Command output was updated to show IPv6 information and to display Resource Reservation Protocol (RSVP) quality of service (QoS) preconditions information.

Usage Guidelines

The **show sip-ua calls** command displays active UAC and UAS information for SIP calls on a Cisco IOS device. The output includes information about IPv6, RSVP, and media forking for each call on the device and for all media streams associated with the calls. There can be any number of media streams associated with a call, of which typically only one is active. However, a call can include up to three active media streams if the call is media-forked. Use this command when debugging multiple media streams to determine if an active call on the device is forked.

Examples

The following is sample output from the **show sip-ua calls** command for a forked call with four associated media streams, three of which are currently active:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID : 515205D4-20B711D6-8015FF77-1973C402@172.18.195.49
 State of the call : STATE_ACTIVE (6)
 Substate of the call : SUBSTATE_NONE (0)
 Calling Number : 5550200
 Called Number : 5551101
 Bit Flags : 0x12120030 0x220000
 Source IP Address (Sig ): 172.18.195.49
 Destn SIP Req Addr:Port : 172.18.207.18:5063
 Destn SIP Resp Addr:Port: 172.18.207.18:5063
 Destination Name : 172.18.207.18
 Number of Media Streams : 4
 Number of Active Streams: 3
 RTP Fork Object : 0x637C7B60
 Media Stream 1
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 28
  Stream Type : voice-only (0)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : inband-voice
```

```
  Dtmf-relay Payload Type : 0
  Media Source IP Addr:Port: 172.18.195.49:19444
  Media Dest IP Addr:Port : 172.18.193.190:16890
 Media Stream 2
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 33
  Stream Type : voice+dtmf (1)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18928
  Media Dest IP Addr:Port : 172.18.195.73:18246
 Media Stream 3
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 34
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18428
  Media Dest IP Addr:Port : 172.16.123.99:34463
 Media Stream 4
  State of the stream : STREAM_DEAD
  Stream Call ID : -1
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:0
  Media Dest IP Addr:Port : 172.16.123.99:0

 Number of UAC calls: 1

SIP UAS CALL INFO

 Number of UAS calls: 0
```

The following is sample output from the **show sip-ua calls** command showing IPv6 information:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID                : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 2000
   Called Number           : 1000
   Bit Flags               : 0xC04018 0x100 0x0
   CC Call ID              : 2
   Source IP Address (Sig ): 2001::21B:D4FF:FED7:B000
   Destn SIP Req Addr:Port : [2001::21B:D5FF:FE1D:6C00]:5060
   Destn SIP Resp Addr:Port: [2001::21B:D5FF:FE1D:6C00]:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
```

```
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO

   Number of SIP User Agent Server(UAS) calls: 0
```

The following is sample output from the **show sip-ua calls** command when mandatory QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

  Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : F31FEA20-CFF411DC-8068DDB4-22C622B8@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:64440
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:18542
  Media Dest IP Addr:Port  : 172.18.19.73:16912
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Mandatory
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success


Options-Ping    ENABLED:NO     ACTIVE:NO
 Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has failed:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
```

```
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Fail

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when the command is used on the originating gateway (OGW) while optional QoS is configured on the OGW, mandatory QoS is configured on the terminating gateway (TGW), and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
```

```
  Stream Type               : voice-only (0)
  Negotiated Codec          : g711ulaw (160 bytes)
  Codec Payload Type        : 0
  Negotiated Dtmf-relay     : inband-voice
  Dtmf-relay Payload Type   : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port   : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                    : -2
  Local QoS Strength        : Optional
  Negotiated QoS Strength   : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status          : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

Table 158 describes the significant fields shown in the displays.

Table 158 show sip-ua calls Field Descriptions

Field	Description
SIP UAC CALL INFO	Field header that indicates that the following information pertains to the SIP UAC.
Call 1	Field header.
SIP Call ID	UAC call identification number.
State of the call	Indicates the state of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Substate of the call	Indicates the substate of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Calling Number	Indicates the calling number.
Called Number	Indicates the called number.
Bit Flags	Indicates the bit flags used for debugging.
Source IP Address (Sig)	Indicates the signaling source IPv4 or IPv6 address.
Destn SIP Req Addr: Port:	Indicates the signaling destination Request IPv4 or IPv6 address and port number.
Destn SIP Resp Addr: Port:	Indicates the signaling destination Response IPv4 or IPv6 address and port number.
Destination Name	Indicates the signaling destination hostname, IPv4 address, or IPv6 address.
Number of Media Streams	Indicates the total number of media streams for this UAC call.
Number of Active Streams:	Indicates the total number of active media streams.
RTP Fork Object	Pointer address of the internal RTP Fork data structure.
Media Stream	Statistics about each active media stream are reported. The Media Stream header indicates the number of the media stream, and its statistics immediately follow this header.

Table 158 show sip-ua calls Field Descriptions (continued)

Field	Description
State of the stream	State of the media stream indicated by the Media Stream header. Can be STREAM_ACTIVE, STREAM_ADDING, STREAM_CHANGING, STREAM_DEAD, STREAM_DELETING, STREAM_IDLE, or Invalid Stream State.
Stream Call ID	Identification of the stream call indicated by the Media Stream header.
Stream Type	Type of stream indicated by the Media Stream header. It can be dtmf-only, dtmf-relay, voice-only, or voice+dtmf-relay.
Negotiated Codec	Codec selected for the media stream. It can be g711ulaw, <G.729>, <G.726>, or No Codec.
Codec Payload Type	Payload type of the Negotiated Codec.
Negotiated Dtmf-relay	DTMF relay selected for the media stream indicated by the Media Stream header. It can be inband-voice or rtp-nte.
Dtmf-relay Payload Type	Payload type of the negotiated DTMF relay.
Media Source IP Addr: Port	The source IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Media Dest IP Addr: Port	The destination IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Local QoS Strength	The QoS strength (mandatory or optional) configured for this device.
Negotiated QoS Strength	The QoS strength (mandatory or optional) that has been negotiated.
Negotiated QoS Direction	Displays the direction in which RSVP was negotiated. For example, sendrecv indicates that RSVP was negotiated in both directions.
Local QoS Status	Displays the success or failure of RSVP reservation.
Number of UAC calls	Final SIP UAC CALL INFO field. Indicates the number of UAC calls.
SIP UAS CALL INFO	Field header that indicates that the following information pertains to the SIP UAS.
Number of UAS calls	Final SIP UAS CALL INFO field. Indicates the number of UAS calls.

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip events	Enablestracing of events that are specific to SIP SPI.
debug ccsip info	Enables tracing of general SIP SPI information.
debug ccsip media	Enables tracing of SIP call media streams.
debug ccsip messages	Enables tracing of SIP Service Provider Interface (SPI) messages.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp** [**tls**] | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all Transport Layer Security (TLS) over TCP connection information.
udp	Displays all User Datagram Protocol (UDP) connection information.
brief	Displays a summary of connections.
detail	Displays detailed connection information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced
12.4(6)T	The optional **tls** keyword was added.
12.4(22)T	Command output was updated to show IPv6 information.
15.1(2)T	The command output was updated to display the SIP socket listeners information.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Examples

The following sample output from this command shows multiple calls to multiple destinations. Although this example shows UDP details, the command output looks identical for TCP calls.

```
Router# show sip-ua connections udp detail

Total active connections : 2
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
```

```
=========== ======= =========== ===========
5060 1 Established 0
Remote-Agent:172.19.154.18, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060        2       Established   0

Router# show sip-ua connections tcp detail

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060         1      Established   0

Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:2001:DB8:C18:4:21D:E5FF:FE34:26A0, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address
  =========== ======= =========== =========== ===========
         5060       2 Established           0  -

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0             [0.0.0.0]:5060
   2             [8.6.8.8]:5060

Router# show sip-ua connections tcp tls brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
```

```
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5061
```

The following is sample output from the **show sip-ua connections** command showing IPv6 information:

```
Router# show sip-ua connections udp brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 10

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5060
```

Table 159 describes the significant fields shown in the display.

Table 159 show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues, and the connection was frequently ended.
No. of remote closures	Indicates the number of times a remote gateway ended the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261-compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were ended or timed out because of signaling inactivity. During call traffic, this number should be zero. If it is not zero, we recommend that the inactivity timer be tuned to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.

Table 159 show sip-ua connections Field Descriptions (continued)

Field	Description
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS software should automatically overcome this condition. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that are marked with "++" at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is not being used. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.

Related Commands

Command	Description
clear sip-ua tcp connection	Clears a SIP TCP connection.
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP user agent status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

show sip-ua map

To display the mapping table of public switched telephone network (PSTN) cause codes and their corresponding Session Initiation Protocol (SIP) error status codes or the mapping table of SIP-to-PSTN codes, use the **show sip-ua map** command in privileged EXEC mode.

show sip-ua map {**pstn-sip** | **sip-pstn** | **sip-request-pstn**}

Syntax Description

pstn-sip	Displays the PSTN cause-code-to-SIP-status-code mapping table.
sip-pstn	Displays the SIP-status-code-to-PSTN-cause-code mapping table.
sip-request-pstn	Display the SIP-requests-PSTN-cause mapping table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.4(22)T	This command was modified. The **sip-request-pstn** keyword was added.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following is sample output from the **show sip-ua map pstn-sip** command:

```
Router# show sip-ua map pstn-sip

PSTN-Cause   Configured        Default
             SIP-Status       SIP-Status
1               404             404
2               404             404
3               404             404
4               500             500
5               500             500
6               500             500
7               500             500
8               500             500
9               500             500
.
.
.
100             500             500
101             500             500
102             408             408
103             500             500
110             500             500
111             400             400
126             500             500
127             500             500
```

The following is sample output from the **show sip-ua map sip-pstn** command:

```
Router# show sip-ua map sip-pstn

SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
400             127             127
401             57              57
402             21              21
403             57              57
404             1               1
405             127             127
406             127             127
407             21              21
408             102             102
409             41              41
410             1               1
.
.
.
600             17              17
603             21              21
604             1               1
606             58              58
```

The following is sample output from the **show sip-ua map request-pstn** command:

```
Router# show sip-request-pstn

SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
CANCEL          16              16
```

Table 160 describes the significant fields shown in the displays.

Table 160 show sip-ua map Field Descriptions

Field	Description
PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Configured SIP-Status	Configured SIP status code or event. SIP Status code range is from 400 to 699.
Default SIP-Status	Default mapping between and PSTN and SIP networks.
SIP-Status	Configured SIP status code or event. SIP status code range is from 400 to 699.
Configured PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Default PSTN-Cause	Default mapping between and SIP and PSTN networks.

Related Commands

Command	Description
set pstn-cause	Sets an incoming PSTN release cause code to a SIP error status code.
set sip-status	Sets an incoming SIP error status code to a PSTN release cause code.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua min-se

To show the current value of the minimum session expiration (Min-SE) header for calls that use the Session Initiation Protocol (SIP) session timer, use the **show sip-ua min-se** command in privileged EXEC mode.

show sip-ua min-se

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(9)T	The Min-SE header default time was changed from 3200 to 90 seconds.

Usage Guidelines

Use this command to verify the value of the Min-SE header.

Examples

The following is sample output from this command:

```
Router# show sip-ua min-se

SIP UA MIN-SE Value (seconds)
Min-SE: 90
```

Table 161 describes the fields shown in this output.

Table 161 show sip-ua min-se Field Descriptions

Field	Description
SIP UA MIN-SE Value (seconds)	Field header indicating that the following information shows the current value of the Min-SE header, in seconds.
Min-SE	Current value of the Min-SE header, in seconds.

Related Commands

Command	Description
min-se (SIP)	Changes the Min-SE header value for all calls that use the SIP session timer.

show sip-ua mwi

To display Session Initiation Protocol (SIP) message-waiting indication (MWI) settings on the voice-mail server, use the **show sip-ua mwi** command in privileged EXEC mode.

show sip-ua mwi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show sip-ua mwi** command:

```
Router# show sip-ua mwi

MWI type: 2
MWI server: dns:unity-vm.gb.com
MWI expires: 60
MWI port: 5060
MWI transport type: UDP
MWI unsolicited
MWI server IP address:
C801011E
0
0
0
0
0
0
0
MWI ipaddr cnt 1:
MWI ipaddr idx 0:
MWI server: 192.168.1.30, port 5060, transport 1
MWI server dns lookup retry cnt: 0
endpoint 8000  mwi status ON
endpoint 8000  mwi status ON
endpoint 8001  mwi status OFF
```

Table 162 provides a listing of the fields in the sample output.

Table 162 show sip-ua mwi Field Descriptions

Field	Description
MWI type	Indicates the type of MWI service. 1 indicates MWI application service, which is used when a router provides MWI relay service. 2 indicates SIP-based MWI.
MWI server	Indicates the host device housing the domain name server (DNS) that resolves the name of the voice-mail server.
MWI expires	Indicates the expiration time, in seconds.
MWI port	Indicates the port used by SIP signaling.
MWI transport type	Indicates the desired transport protocol. Values are tcp or udp. UDP is the default.
MWI unsolicited	Indicates whether unsolicited MWI is configured.
MWI server IP address	Indicates the IP address of the voice-mail MWI server in hex format. If you configured the **mwi-server** command for DNS format, DNS lookup may result in multiple IP addresses. All IP addresses are listed.
MWI ipaddr cnt	Indicates the number of IP addresses associated with the voice-mail MWI server.
MWI ipaddr idx	Indicates which MWI server IP address is currently being used. The index starts from 0.
MWI server	Indicates the IP address of the MWI server; the port; and transport protocol (1 indicates UDP; 2 indicates TCP).
MWI server dns lookup retry cnt	Indicates the number of retries for DNS lookup.
endpoint / mwi status	Indicates the endpoint or voice port and whether MWI notification is active. That is, if a message is waiting, the status is on. Once the message is deleted, the status is off.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua register status

To display the status of E.164 numbers that a Session Initiation Protocol (SIP) gateway has registered with an external primary SIP registrar, use the **show sip-ua register status** command in privileged EXEC mode.

show sip-ua register status [**secondary**]

Syntax Description

secondary	(Optional) Displays the status of E.164 numbers that a SIP gateway has registered with an external secondary SIP registrar.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

SIP gateways can register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar. The command **show sip-ua register status** is only for outbound registration, so if there are no SCCP phones or FXS dialpeers to register, there is no output when the command is run.

Examples

The following is sample output from this command:

```
Router# show sip-ua register status

Line peer expires(sec) registered
4001 20001 596         no
4002 20002 596         no
5100 1     596         no
9998 2     596         no
```

Table 163 describes significant fields shown in this output.

Table 163 show sip-ua register status Field Descriptions

Field	Description
Line	The phone number to register.
peer	The registration destination number.
expires (sec)	The amount of time, in seconds, until registration expires.
registered	Registration status.

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.

show sip-ua retry

To display retry statistics for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua retry** command in privileged EXEC mode.

show sip-ua retry

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/reliable 1*xx*), Conditions met (COMET) responses, and Notify responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command found previously in this reference.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and the Cisco AS5400 in this release.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from this command.

```
Router# show sip-ua retry

SIP UA Retry Values
invite retry count = 6 response retry count = 1
bye retry count = 1 cancel retry count = 1
prack retry count = 10 comet retry count = 10
reliable 1xx count = 6 notify retry count = 10
```

Table 164 describes significant fields shown in this output, in alphabetical order.

Table 164 show sip-ua retry Field Descriptions

Field	Description
bye retry count	Number of times that a Bye request is retransmitted.
cancel retry count	Number of times that a Cancel request is retransmitted.
comet retry count	Number of times that a COMET request is retransmitted.
invite retry count	Number of times that an Invite request is retransmitted.
notify retry count	Number of times that a Notify message is retransmitted.
prack retry count	Number of times that a PRACK request is retransmitted.
refer retry count	Number of times that a Refer request is retransmitted.
reliable 1*xx* count	Number of times that a Reliable 1*xx* request is retransmitted.
response retry count	Number of times that a Response request is retransmitted.
SIP UA Retry Values	Field header for SIP UA retry values.

Related Commands

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry rel1xx	Configures the number of times the reliable 1*xx* response is retransmitted.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua service

To display Session Initiation Protocol (SIP) user-agent (UA) service information, use the **show sip-ua service** command in privileged EXEC mode.

show sip-ua service

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples The following example displays output when SIP UA call service is enabled:

```
Router# show sip-ua service

SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip-ua service

SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip-ua service

SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is stopped forcefully with the **call service stop forced** command:

```
Router# show sip-ua service

SIP service is forced shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is forcefully shutdown globally with the **shutdown forced** command:

```
Router# show sip-ua service

SIP service is forced shut globally
under 'voice service voip'
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
call service stop	Shuts down VoIP call service on a gateway.
voice service	Enters voice-service configuration mode and specifies a voice-encapsulation type.

show sip-ua statistics

To display response, traffic, and retry Session Initiation Protocol (SIP) statistics, use the **show sip-ua statistics** command in privileged EXEC mode.

show sip-ua statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced as follows: BadRequest counter (400 class) now counts malformed Via entries, reliable provisional responses (PRACK/rel1*xx*), conditions met (COMET), and NOTIFY responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Command output was enhanced as follows: • OkInfo counter (200) class counts the number of successful responses to INFO requests. • Info counter counts the number of INFO messages received and sent. • BadEvent counter (489 response) counts responses to Subscribe messages with event types that are not understood by the server. • OkSubscribe counter (200 class) counts the number of 200 OK SIP messages received and sent in response to Subscribe messages. • Subscribe requests indicate total requests received and sent. • SDP application statistics added to monitor SDP. This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Release	Modification
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T. The following cause codes were obsoleted from the command output: • Redirection code: *SeeOther* • Client Error: *LengthRequired* A new SIP statistics counter was added: • Miscellaneous Counters: *RedirectResponseMappedToClientError* Command output was enhanced to display the following: • Time stamp that indicates the last time that SIP statistics counters were cleared.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
12.2(15)ZJ	Command output was enhanced to display the following: • Register counter and statistics.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Command output was enhanced to display SUBSCRIBE retry statistics.

Usage Guidelines

Use the **show sip-ua statistics** command to verify SIP configurations.

Examples

The following is sample output from this command:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
     Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkSubscribe 0/0, OkNOTIFY 0/0,
      OkInfo 0/0, 202Accepted 0/0
      OkRegister 12/49
     Redirection (Inbound only except for MovedTemp(Inbound/Outbound)) :
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0/0, UseProxy 0,
      AlternateService 0
      Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, BadExtension 0/0,
      TempNotAvailable 0/0, CallLegNonExistent 0/0,
      LoopDetected 0/0, TooManyHops 0/0,
      AddrIncomplete 0/0, Ambiguous 0/0,
      BusyHere 0/0, RequestCancel 0/0,
```

```
      NotAcceptableMedia 0/0, BadEvent 0/0,
      SETooSmall 0/0

     Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
     Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
      Miscellaneous counters:
      RedirectRspMappedToClientErr 0

SIP Total Traffic Statistics (Inbound/Outbound)
      Invite 0/0, Ack 0/0, Bye 0/0,
      Cancel 0/0, Options 0/0,
      Prack 0/0, Comet 0/0,
      Subscribe 0/0, NOTIFY 0/0,
      Refer 0/0, Info 0/0
      Register 49/16

Retry Statistics
      Invite 0, Bye 0, Cancel 0, Response 0,
      Prack 0, Comet 0, Reliable1xx 0, Notify 0
      Register 4, Subscribe 0

SDP application statistics:
Parses: 0, Builds 0
Invalid token order: 0, Invalid param: 0
Not SDP desc: 0, No resource: 0

Last time SIP Statistics were cleared: <never>
```

Command output, listed in Table 165, includes a reason phrase and a count describing the SIP messages received and sent. When x/x is included in the reason phrase field, the first number is an inbound count, and the second number is an outbound count. The description field headings are based on the SIP response code xxx, which the SIP protocol uses in determining behavior. SIP response codes are classified into one of the following six categories:

- 1*xx*: Informational, indicates call progress.
- 2*xx*: Success, indicates successful receipt or completion of a request.
- 3*xx*: Redirection, indicates that a redirect server has returned possible locations.
- 4*xx*: Client error, indicates that a request cannot be fulfilled as it was submitted.
- 5*xx*: Server error, indicates that a request has failed because of an error by the server. The request may be retried at another server.
- 6*xx*: Global failure, indicates that a request has failed and should not be tried again at any server.

Table 165 describes significant fields shown in this output, in alphabetical order.

Table 165 show sip-ua statistics Field Descriptions

Field	Description
Note For each field, the standard RFC 2543 SIP response number and message are shown.	
Ack 0/0	A confirmed final response received or sent.
Accepted 0/0	202 A successful response to a Refer request received or sent.

Table 165 show sip-ua statistics Field Descriptions (continued)

Field	Description
AddrIncomplete 0/0	484 Address supplied is incomplete.
AlternateService 0	380 Unsuccessful call; however, an alternate service is available.
Ambiguous 0/0	485 Address supplied is ambiguous.
BadEvent 0/0	489 Bad Event response indicates a Subscribe request having an event type that the server could not understand.
BadExtension 0/0	420 Server could not understand the protocol extension in the Require header.
BadGateway 0/0	502 Network is out of order.
BadRequest	400 Bad Request (includes the malformed Via header).
BadSipVer 0/0	505 Requested SIP version is not supported.
BusyEverywhere 0/0	600 Called party is busy.
BusyHere 0/0	486 Called party is busy.
Bye 0	Number of times that a Bye request is retransmitted to the other user agent.
Bye 0/0	Terminated the session.
CallLegNonExistent 0/0	481 Server is ignoring the request. Either is was a Bye request and there was no matching leg ID, or it was a Cancel request and there was no matching transaction.
Cancel 0	Number of times that a Cancel request is retransmitted to the other user agent.
Cancel 0/0	Terminated the pending request.
Comet 0	Number of times that a COMET request is retransmitted to the other user agent.
Comet 0/0	Conditions have been met.
Conflict 0/0	409 Temporary failure.
Decline 0/0	603 Call rejected.
Forbidden 0/0	403 The SIP server has the request, but cannot provide service.
Forwarded 0/0	181 Call has been forwarded.
GatewayTimeout 0/0	504 The server or gateway did not receive a timely response from another server (such as a location server).
Gone 0/0	410 Resource is no longer available at the server, and no forwarding address is known.
Info 0/0	Number of information messages the gateway has received (inbound) and how many have been transmitted (outbound).
InternalError 0/0	500 The server or gateway encountered an unexpected error that prevented it from processing the request.
Invite 0	Number of times that an INVITE request is retransmitted to the other user agent.
Invite 0/0	Initiates a call.

Table 165 show sip-ua statistics Field Descriptions (continued)

Field	Description
LoopDetected 0/0	482 A loop—server received a request that included itself in the path.
MethodNotAllowed 0/0	405 Method specified in the request is not allowed.
MovedPermanently 0	301 User is no longer available at this location.
MovedTemporarily 0	302 User is temporarily unavailable.
MultipleChoice 0	300 Address resolves to more than one location.
NotAcceptable 0/0	406/606 Call was contacted, but some aspect of the session description was unacceptable.
NotAcceptableMedia 0/0	406 Call was contacted, but some aspect of the session description was unacceptable.
NotExistAnywhere 0/0	604 Server has authoritative information that the called party does not exist in the network.
NotFound 0/0	404 Called party does not exist in the specified domain.
NOTIFY 0	Number of times that a Notify is retransmitted to the other user agent.
NOTIFY 0/0	Number of Notify messages received or sent.
NotImplemented 0/0	501 Service or option not implemented in the server or gateway.
OkBye 0/0	200 Successful response to a Bye request.
OkCancel 0/0	200 Successful response to a Cancel request.
OkInfo	200 Successful response to an INFO request.
OkInvite 0/0	200 Successful response to an INVITE request.
OkNOTIFY 0/0	200 Successful response to a Notify request.
OkOptions 0/0	200 Successful response to an Options request.
OkPrack 0/0	200 Successful response to a PRACK request.
OkPreconditionMet 0/0	200 Successful response to a PreconditionMet request.
OkRegister 0/0	200 Successful response to a Register request.
OkSubscribe 0/0	200 Successful response to a SUBSCRIBE request.
Options 0/0	Query the receiving or sending server as to its capabilities.
PaymentRequired 0/0	402 Payment is required to complete the call.
Prack 0	Number of times that a PRACK request is retransmitted to the other user agent.
Prack 0/0	Provisional response received or sent.
PreCondFailure 0/0	580 The session could not be established because of failure to meet required preconditions.
ProxyAuthReqd 0/0	407 Rejected for proxy authentication.
Queued 0/0	182 Until the called party is available, the message is queued.

Table 165 show sip-ua statistics Field Descriptions (continued)

Field	Description
RedirectResponseMappedTo ClientError 0	Indicates the count of incoming 3*xx* responses that were mapped to 4*xx* responses. It is incremented when the **no redirection** command is active. For the default case, the 3*xx* messages are processed per RFC 2543, and this counter is not incremented. This counter counts only inbound messages and only the 3*xx* responses that are known (300, 301, 302, 305, and 380). The counter is cleared when the **clear sip-ua statistics** command is issued.
Refer 0	Number of times the Refer request is retransmitted to the other user agent.
Refer 0/0	Number of Refer requests received or sent.
Register 0/0	Number of Register requests received or sent.
Register 0	Number of times that a Register request is retransmitted to the other user agent.
Reliable1xx 0	Indicates the number of times the Reliable 1*xx* response is retransmitted to the other user agent.
ReqEntityTooLarge 0/0	413 Server refuses to process request because the request is larger than is acceptable.
ReqTimeout 0/0	408 Server could not produce a response before the Expires time- out.
RequestCancel 0/0	Request has been canceled.
ReqURITooLarge 0/0	414 Server refuses to process, because the URI (URL) request is larger than is acceptable.
Response 0	Indicates number of Response retries.
Retry Statistics	One of the three categories of response statistics.
Ringing 0/0	180 Called party has been located and is being notified of the call.
SeeOther 0	303 Transfer to another address.
ServiceUnavail 0/0	503 Service option is not available because of an overload or maintenance problem.
SessionProgress 0/0	183 Indicates in-band alerting.
SIP Response Statistics (Inbound/Outbound)	One of the three categories of response statistics.
SIP Total Traffic Statistics (Inbound/Outbound)	One of the three categories of response statistics.
Subscribe 0	Indicates the number of Retry Subscribe messages sent.
Subscribe 0/0	Number of Subscribe requests received or sent.
TempNotAvailable 0/0	480 Called party did not respond.
TooManyHops 0/0	483 A server received a request that required more hops than is allowed by the Max-Forward header.
Trying 0/0	100 Action is being taken with no resolution.
Unauthorized 0/0	401 The request requires user authentication.

Table 165 show sip-ua statistics Field Descriptions (continued)

Field	Description
UnsupportedMediaType 0/0	415 Server refuses to process a request because the service option is not available on the destination endpoint.
UseProxy 0	305 Caller must use a proxy to contact called party.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua status

To display status for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua status** command in privileged EXEC mode.

show sip-ua status

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The statistics portion of the output was removed and included in the **show sip-ua statistics** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display if media or signaling binding is enabled, and the style of the DNS SRV query (1 for RFC 2052; 2 for RFC 2782).
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	Command output was enhanced to display information on Session Description Protocol (SDP) application configuration. This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T	Command output was enhanced to display the following: Information on redirection message handling. Information on handling of 180 responses with SDP.
12.2(15)T	Command output was enhanced to display Suspend and Resume support.
12.2(15)ZJ	Command output was enhanced to display information on the duration of dual-tone multifrequency (DTMF) events.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display Reason Header support.
12.4(22)T	Command output was updated to show IPv6 information.
Cisco IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines Use this command to verify SIP configurations.

Examples

The following is sample output from the **show sip-ua status** command:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4

SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The following is sample output from the **show sip-ua status** command showing IPv6 information:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6

SDP application configuration:
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
```

```
Network types supported: IN
Address types supported: IP4 IP6
Transport types supported: RTP/AVP udptl
```

Table 166 describes the significant fields shown in the display.

Table 166 show sip-ua status Field Descriptions

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	User Datagram Protocol (UDP) is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP early-media for 180 responses with SDP	Early media cut-through treatment for 180 responses with SDP can be enabled (the default treatment) or disabled, with local ringback provided.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of the DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.
NAT Settings for the SIP-UA	Symmetric Network Address Translation (NAT) settings when the feature is enabled.
Role in SDP	Identifies the endpoint function in the connection setup procedure during symmetric NAT traversal. The endpoint role may be set to active, meaning that it initiates a connection, or to passive, meaning that it accepts a connection. A value of none in this field means that the feature is disabled.
Check media source packets	Media source packet checking is enabled or disabled.
Maximum duration for a telephone-event in NOTIFYs	Shows the time interval, in milliseconds (ms), between consecutive NOTIFY messages for a telephone event.
SIP support for ISDN SUSPEND/RESUME	Suspend and Resume support is enabled or disabled.
Redirection (3xx) message handling	Redirection can be enabled, which is the default status, according to RFC 2543. Or handling of redirection 3*xx* messages can be disabled, allowing the gateway to treat 3*xx* redirect messages as 4*xx* error messages.
Reason Header will override Response/Request Codes	Reason header is enabled or disabled.
protocol mode is ipv6	States whether the protocol being used is IPv6 or IPv4.
Version line (v=)	Indicates if the SDP version is required.
Owner line (o=)	Indicates if the session originator is required.
Timespec line (t=)	Indicates if the session start and stop times are required.
Media supported	Media information.
Network types supported	Always IN for Internet.

Table 166 show sip-ua status Field Descriptions (continued)

Field	Description
Address types supported	Identifies the Internet Protocol version.
Transport types supported	Identifies the transport protocols supported.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua status refer-ood

To display the number of incoming and outgoing out-of-dialog REFER (OOD-R) connections, use the **show sip-ua status refer-ood** command in privileged EXEC mode.

show sip-ua status refer-ood

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use this command to verify OOD-R processing.

Examples

The following is sample output from the **show sip-ua status refer-ood** command:

```
Router# show sip-ua status refer-ood

Maximum allow incoming out-of-dialog refer 500
Current existing incoming out-of-dialog refer dialogs: 1
                  outgoing out-of-dialog refer dialogs: 0
```

Table 166 describes significant fields shown in this output.

Table 167 show sip-ua status refer-ood Field Descriptions

Field	Description
Maximum allow incoming out-of-dialog refer	Maximum number of incoming OOD-R sessions that the router is allowed. Value set by the **refer-ood enable** command. Default is 500.
Current existing incoming out-of-dialog refer dialogs	Number of currently active incoming OOD-R sessions.
outgoing out-of-dialog refer dialogs	Number of currently active outgoing OOD-R sessions used for line status updates.

Related Commands

Command	Description
refer-ood enable	Enables OOD-R processing.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua timers

To display the current settings for the Session Initiation Protocol (SIP) user-agent (UA) timers, use the **show sip-ua timers** command in privileged EXEC mode.

show sip-ua timers

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The output of this command was changed to reflect the various forms of the **timers** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/rel 1*xx*), Conditions met (COMET), and NOTIFY responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command found previously in this reference.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)YT	Command output was enhanced to display Refer responses.
12.2(15)T	This command was supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
12.3(1)	Command output was enhanced to display the SIP hold timer value.
12.2(15)ZJ	Command output was enhanced to display Register responses.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display the buffer-invite timer value and the connection aging timer value.

Usage Guidelines Use this command to verify SIP configurations.

Examples

The following is sample output from this command:

```
Router# show sip-ua timers

SIP UA Timer Values (millisecs)
trying 500, expires 150000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500, refer 500, register 500
hold 2880 minutes, buffer-invite 500, aging 5 minutes
```

Table 168 describes significant fields shown in this output.

Table 168 show sip-ua timers Field Descriptions

Field	Description
SIP UA Timer Values (millisecs)	SIP UA timer status.
trying	Time to wait before a Trying message is retransmitted.
expires	Time to wait before an Expires message is retransmitted.
connect	Time to wait before a Connect message is retransmitted.
disconnect	Time to wait before a Disconnect message is retransmitted.
comet	Time to wait before a COMET message is retransmitted.
prack	Time to wait before a PRACK acknowledgment is retransmitted.
rel1xx	Time to wait before a Rel1*xx* response is retransmitted.
notify	Time to wait before a Notify response is retransmitted.
refer	Time to wait before a Retry request is retransmitted.
register	Time to wait before a Register request is retransmitted.
hold	Time to wait in minutes before a BYE request is sent.
buffer-invite	Time to buffer the INVITE while waiting for display information.
aging	Time to wait in minutes before a TCP or UDP connection is aged out.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
sip-ua	Enables the SIP user-agent configuration commands.

show spe voice

To display voice-service-history statistics for a specified service processing element (SPE), use the **show spe voice** command in privileged EXEC mode.

show spe voice {[**active**] {*slot* | *slot*/*spe*} | **summary** [*slot* | *slot*/*spe*]}

Syntax Description

slot	All SPEs on the specified slot. Cisco AS5350 range: 1 to 3. Cisco AS5400 range: 1 to 7. Cisco AS5850 range: 0 to 13.
slot/*spe*	Specified SPE on the specified slot. Slot range: as above. SPE range as follows: • Cisco 5350 and Cisco 5400: 0 to 17 • Cisco 5850 (in a CT3_UP216 card): 0 to 35 • Cisco 5850 (in a UP324 card): 0 to 53 You must include the slash mark.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the *slot* or *slot*/*spe* argument once to specify a single slot or SPE. Use it twice to specify the first and last of a range of slots or SPEs.

The following examples specify the following: a single SPE, a single slot, a range of SPEs in a slot, and a range of slots:

```
show spe voice 1/3
show spe voice 1
show spe voice 1/1 1/3
show spe voice 1 3
```

The **summary** keyword permits you to employ output modifiers to the command so as to write large amounts of data output directly to a file for later reference. You can save this file on local or remote storage devices such as flash, a SAN disk, or an external memory device. You can write output to a new file or append it to an existing file and, optionally at the same time, display it onscreen. Redirection is available using a pipe (|) character combined with the **redirect**, **append**, or **tee** keywords.

For more information on output modifiers, see *Show Command Output Redirection* at the following location: http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_s08.html#wp1378339

Examples

The following example shows information for a single SPE (slot 2, SPE 1):

```
Router# show spe voice 2/1

#SPE 2/01
Cisco Universal SPE (Managed); Port 2/6 - 2/11
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection Errors
         0 Bad Protocol Headers

Codec          Calls   Codec     Calls   Codec           Calls   Codec     Calls
G.711 u-Law        0   G.729         0   G.723.1 6.3K        0   GSM FR        0
G.711 a-Law        0   G.729B        0   G.723.1 5.3K        0   GSM HR        0
G.726 40K          0   G.729A        0   G.723.1A 6.3K       0   GSM EFR       0
G.726 32K          0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K          0   G.728         0   Clear Channel       0
G.726 16K          0
```

The following example shows summary information:

```
Router# show spe voice summary

Cisco Universal SPE (Managed); Port 1/0 - 1/107
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection
Errors
         0 Bad Protocol Headers

Codec          Calls   Codec     Calls   Codec           Calls   Codec       Calls
G.711 u-Law        0   G.729         0   G.723.1 6.3K        0   GSM FR      0
G.711 a-Law        0   G.729B        0   G.723.1 5.3K        0   GSM HR      0
G.726 40K          0   G.729A        0   G.723.1A 6.3K       0   GSM EFR     0
G.726 32K          0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K          0   G.728         0   Clear Channel       0   G.726 16K   0
```

Table 169 describes the significant fields shown in the display.

Table 169 show spe voice Command Field Descriptions

Field	Description
SPE	Slot and port number of the SPE.
Last Clearing of Statistics Counters	Last time the statistics counters were cleared by means of the **clear spe counters** command.
Buffer Overflow Errors	The digital-signal-processor (DSP) buffer has overflowed. If overflow continues, data will be lost and voice will be distorted (as concealment is added).

Table 169 show spe voice Command Field Descriptions (continued)

Field	Description
Endpoint Detection Errors	A voice frame has arrived after a predefined timer expires, causing the DSP to declare it late. If the frame consists of the SID/marker bit, it causes an endpoint detection error and the late packet is included as an endpoint detection error.
Packets Received Early	The number of frames held in the delay buffer exceeds the expected playout delay — that is, the delay buffer is overrun (too many frames waiting to be played out for the expected playout delay). At this point, the buffer must reduce the excess delay using intelligent frame deletion to preserve audio continuity.
Packets Received Late	The DSP has received an out-of-sequence packet and started a timer for the missing packet. The packet has failed to arrive in time; it is marked as late and the statistic is incremented. The DSP does interpolative or silence concealment for any missing frames. This type of problem is apt to occur in a congested network and results in lost packets and diminished voice quality.
Bad Protocol Headers	Packets have been rejected for any of the following reasons: bad protocol header, incorrect length, unknown packet format, unknown Real-Time Transport Protocol synchronization source (SSRC), incorrect checksum (when the Extended header is used), cumulative number of packets with invalid RTP headers (the header extension exceeds the packet length), or an invalid User Datagram Protocol (UDP)/IP header if extended encapsulation is enabled.

Related Commands

Command	Description
show spe	Displays SPE status.
show spe modem	Displays modem service-history statistics for a specified SPE.
show spe version	Displays the firmware version on a specified SPE.

show ss7 mtp1 channel-id

To display information for a given session channel ID, use the **show ss7 mtp1 channel-id** command in privileged EXEC mode.

show ss7 mtp1 channel-id [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 23.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command is useful for determining which channel IDs have already been allocated.

Examples

The following sample output displays the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started:

```
Router# show ss7 mtp1 channel-id

  SS7 MTP1 Session-channel [all]:
       channel  assigned interface
       -------  ------------------
           0      7/0:0  (digital)
           1        7/0   (serial)
           3      7/0:1  (digital)
```

Table 170 describes significant fields shown in this output.

Table 170 show ss7 mtp1 channel-id Field Descriptions

Field	Description
SS7 MTP1 Session-channel	Information about channel IDs.
all	Information on all assigned channel IDs if a particular ID is not specified.
channel	Channel ID assigned by use of the **channel-id** command.
assigned	Name of the interface serial object to which the channel ID is assigned.
interface	Whether the link type is digital or serial.

The following sample output concerns a specified channel-ID parameter:

```
Router# show ss7 mtp1 channel-id 1

serial interface:  7/0:1 (digital)
  SCC port:          2
  link state:        STARTED
  IDB state:         IDBS_UP

  rcv-pool:
     pool-name:      Rcv07:02
     congested:      FALSE
     in-use buffers: 16
     free buffers:   384

  tx-pool:
     pool-name:      SS7txB01
     in-use buffers: 64
     free buffers:   1236
```

Table 171 describes significant fields shown in this output.

Table 171 show ss7 mtp1 channel-id Field Descriptions (Specific Channel-ID Selected)

Field	Description
serial interface	Name of the interface serial object and its type (serial or digital).
SCC port	SCC port on the DFC card that was internally assigned by software to service that link (useful to resolve conflicts when trying to create a serial link).
link state	MTP1 link state is started (generally reflects the shutdown and no shutdown entry options.
IDB state	Actual state of the internal Interface Descriptor Block (IDB), which is useful for developers.
rcv-pool	Heading for receive buffer-pool information.
pool-name	Internal name for the pool.
congested	Whether the receive buffers are congested or not.
in-use buffers	How many of the receive buffers are currently in use.
free buffers	How many of the receive buffers are free (not in use).
tx-pool	Heading for transmit buffer-pool information.
pool-name	Internal name for the pool.
in-use buffers	How many of the transmit buffers are currently in use.
free buffers	How many of the transmit buffers are free (not in use).

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.
show ss7 mtp2 ccb	Displays SS7 MTP 2 Channel Control Block (CCB) information.
show ss7 mtp2 state	Displays internal SS7 Message Transfer Part level 2 (MTP 2) state machine information.

Command	Description
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP 2 protocol variant.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp1 links

To display information for each provisioned Signaling System 7 (SS7) link, use the **show ss7 mtp1 links** command in privileged EXEC mode.

show ss7 mtp1 links

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	This command was implemented on the Cisco 2600 series. Command output was also modified.

Usage Guidelines

Use this command to display the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started. This command is useful for quickly letting you know what links have been assigned and what channel IDs are in use.

The output for this command has been modified for the Cisco AS5350 and Cisco AS5400 to show SS7 session set information. For the Cisco 2600 series, the SCC and state columns have been removed from the output.

Examples

The following sample output shows that there are four SS7 links (out of a platform maximum of four).

Note The SCC chip number is used by Cisco developers who are checking output from the **debug ss7 mtp1** commands.

```
Router# show ss7 mtp1 links

     SS7 MTP1 Links [num = 4, platform max = 4]:

                                          session
       interface  type      SCC  state    channel
       ---------  --------  ---  -------  -------
       7/0:0      digital   7/3  STARTED  0
       7/0:1      digital   7/2  STARTED  1
       7/1:0      digital   7/1  STARTED  2
       7/1:1      digital   7/0  STARTED  3
```

The following example displays the interface, type (serial or digital), SCC port, state (started or stopped), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco AS5350 or Cisco AS5400.

```
Router# show ss7 mtp1 links
```

```
SS7 MTP1 Links [num = 4, platform max = 4]:

                                          session session
  interface   type   SCC     state        channel   set
  --------- -------- --- ------------ ------- -------
     7/0:0  digital  7/3      STARTED     1       0
     7/0:1  digital  7/2      STOPPED    NA      NA
     7/0:2  digital  7/1      STARTED     3       0
       7/0   serial  7/0      STARTED     0       0
```

The following example displays the interface, type (serial or digital), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco 2611 or Cisco 2651. The SCC and state columns have been removed from the output for these platforms.

```
Router# show ss7 mtp1 links

SS7 MTP1 Links [num = 4, platform max = 4]:

                      session session
   interface   type   channel   set
   --------- -------- ------- -------
        0/0   serial      0       0
        0/1   serial      1       0
      0/2:0  digital      2       1
      0/3:0  digital      3       1
```

Table 172 describes significant fields shown in this output.

Table 172 show ss7 mtp1 links Field Descriptions

Field	Description
interface	Name of the serial interface for the link.
type	Type of link: serial or digital.
SCC	Assigned MGC port. The SCC chip number is used by Cisco developers to check output from the **debug ss7 mtp1** command.
State	Whether the link is stopped or started.
channel	Assigned channel ID.
session channel	Assigned channel ID.
session set	Assigned SS7 session number.

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB-information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP2 state machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

Command	Description
show ss7 sm session	Displays information about an SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp2 ccb

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) call-control block (CCB) information, use the **show ss7 mtp2 ccb** command in privileged EXEC mode.

show ss7 mtp2 ccb [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0

Command Default

Channel 0. The default is set when you first configure the MTP2 variant. The link must be out of service when you change the variant.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	The command output was modified to display the following new parameters for the PCR feature: PCR enabled, N2, forced retransmission, and octet count.

Usage Guidelines

The application and meaning of the output is dependent on the MTP2 variant. For example, Japanese Nippon Telephone and Telegraph Cellular System (NTT) and the Japanese Telecommunications Technology Committee (TTC) support only emergency alignment.

Examples

The following is sample output from this command. Output highlighted in bold is for the PCR feature.

```
Router# show ss7 mtp2 ccb 0

SS7 MTP2 Internal Channel Control Block Info for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997

ModuloSeqNumber             = 128   (0x80  )
MaxSeqNumber                = 127   (0x7F  )
Unacked-MSUs (MaxInRTB)     = 127   (0x7F  )
MaxProvingAttempts          = 5     (0x5   )
error_control               = Basic
LSSU_Len                    = 1     (0x1   )
MSU_Len                     = 272   (0x110 )

SUERM-threshold             = 64    (0x40  )
SUERM-number-octets         = 16    (0x10  )
SUERM-number-SUs            = 256   (0x100 )

Tie-AERM-Emergency          = 1     (0x1   )
Tin-AERM-Normal             = 4     (0x4   )
```

```
MSU_FISU_Accepted_flag      = TRUE
LSSU_available              = TRUE
AbnormalBSN_flag            = FALSE
AbnormalBSN_flag            = FALSE
UnreasonableBSN             = FALSE
UnreasonableFSN             = FALSE
Abnormal_FIBR_flag          = FALSE
congestionDiscard           = FALSE

ThisIsA_MSU                 = FALSE
local_processor_outage      = FALSE
remote_processor_outage     = FALSE

provingEmergencyFlag        = TRUE
RemoteProvingEmergencyFlag  = FALSE
further_proving_required    = FALSE

ForceRetransmitFlag         = FALSE
RetransmissionFlag          = FALSE

link_present                = TRUE
Debug Mask                  = 0x0


TX Refc RTB Busy            = 0
TX Refc XTB Fault           = 0
TX Too Long Lost            = 0
TX Enqueue Too Large        = 0
TX Enqueue Failed           = 0
TX CountRTBSlotFull         = 0
TX MaxMSUinXTB              = 0
PCR Enabled                   = TRUE
Forced Retransmission Enabled = TRUE
Forced Retransmission Counts  = 0
N2 Threshhold                 = 4500 octets
N2 Octet-count                = 0 octets

SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997

OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0

OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0

OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0

OMLSSU_XMIT_Count       = 6670
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 6670
OMLSSU_XMIT_SIOSCount   = 0
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0

OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
```

```
OMLSSU_RCV_SIECount      = 0
OMLSSU_RCV_SIOCount      = 0
OMLSSU_RCV_SIOSCount     = 0
OMLSSU_RCV_SIPOCount     = 0
OMLSSU_RCV_SIBCount      = 0
OMLSSU_RCV_InvalidCount  = 0

OMRemote_PO_Count        = 0
OMRemote_Congestion_Cnt  = 0

OMtimeINSV (secs)        = 0
OMtimeNotINSV (secs)     = 8
OMMSUBytesTransmitted    = 0
OMMSUBytesReceived       = 0

OMTransmitReqCount       = 7678
OMPDU_notAcceptedCount   = 0
OMPDU_NACK_Count         = 0
OMunreasonableFSN_rcvd   = 0
OMunreasonableBSN_rcvd   = 0

OMT1_TMO_Count           = 0
OMT2_TMO_Count           = 1
OMT3_TMO_Count           = 0
OMT4_TMO_Count           = 0
OMT5_TMO_Count           = 0
OMT6_TMO_Count           = 0
OMT7_TMO_Count           = 0
OMT8_TMO_Count           = 0
OMTA_TMO_Count           = 0
OMTF_TMO_Count           = 0
OMTO_TMO_Count           = 0
OMTS_TMO_Count           = 0
OMLostTimerCount         = 0

OMOMLostBackHaulMsgs     = 0

OMAERMCount              = 0
OMAERMFailCount          = 0
OMSUERMCount             = 0
OMSUERMFailCount         = 0
OMCongestionCount        = 0
OMCongestionBackhaulCnt  = 0
```

Table 173 describes significant fields shown in this output.

Table 173 show ss7 mtp2 ccb Field Descriptions

Field	Description	Possible Values
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE indicates that PCR is enabled. FALSE indicates that PCR is disabled.

Table 173 show ss7 mtp2 ccb Field Descriptions (continued)

Field	Description	Possible Values
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE indicates that forced-retransmission is enabled. FALSE indicates that forced-retransmission is disabled.
N2 Threshold N2 Octet-count	Status of the N2 parameter and maximum octets available. Number of octets stored in the RTB for an SS7 signaling channel.	—

Related Commands

Command	Description
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

show ss7 mtp2 state

To display internal Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine information, use the **show ss7 mtp2 state** command in privileged EXEC mode.

show ss7 mtp2 state [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0.

Command Default Information for all channels is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	The command output was modified to display the following new parameters: PCR enabled and forced retransmission.

Examples The following example displays the current state of forced retransmission and PCR-enabled flags (shown in bold in the output below):

```
Router# show ss7 mtp2 state 0

SS7 MTP2 states for channel 0
Protocol version for channel 0 is ITU-T Q.703 (1996) (White Book)
  MTP2LSC_INSERVICE       MTP2IAC_IDLE
  MTP2TXC_INSERVICE       MTP2RC_INSERVICE
  MTP2SUERM_MONITORING    MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
Forced Retransmission    = FALSE
PCR Enabled              = TRUE
N2                       = 800
```

The following is sample output from this command displaying MTP2 state machine information for two different channels:

```
Router# show ss7 mtp2 state 0

SS7 MTP2 states for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS             MTP2IAC_IDLE
  MTP2TXC_INSERVICE       MTP2RC_IDLE
  MTP2SUERM_IDLE          MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

```
Router# show ss7 mtp2 state 1

SS7 MTP2 states for channel 1
Protocol version for channel 1 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS              MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_IDLE
  MTP2SUERM_IDLE           MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul   = Abate
Remote Processor Outage   = FALSE
```

Table 174 describes significant fields shown in this output.

Table 174 show ss7 mtp2 state Field Descriptions

State	Description	Possible Values
MTP2LSC	Overall status of the link.	OOS—Link is out of service. INITIAL_ALIGNMENT—Link is in a transitional link alignment state. ALIGNED_READY—Link is in a transitional link alignment state. ALIGNED_NOT_READY—Link is in a transitional link alignment state. INSERVICE—Link is in service. PROCESSOR_OUTAGE—There is an outage in the local processor. This state implies that the link has been aligned. POWER_OFF—It is possible you don't have the I/O memory set to at least 40 percent. There may not be enough memory for the SS7 MTP2 signaling.
MTP2IAC	Status of the initial alignment control state machine.	IDLE—State machine is idle. It is not aligning the link. NOT_ALIGNED—State machine has begun the alignment process. ALIGNED— Link has exchanged the alignment handshake with the remote device. PROVING—Link alignment is being proven. This is a waiting period before the LSC state changes to INSERVICE.
MTP2TXC	Status of the transmission control state machine.	IDLE—State machine is inactive. INSERVICE—State machine is the active transmitter.
MTP2RC	Status of the receive control state machine.	IDLE—State machine is inactive. INSERVICE—State machine is the active receiver.

Table 174 show ss7 mtp2 state Field Descriptions (continued)

State	Description	Possible Values
MTP2SUERM	Status of the signal unit error monitor (SUERM).	IDLE—State machine is inactive. MONITORING—SUERM is active. SUERM uses a leaky-bucket algorithm to track link errors while the link is in service. If the number of link errors reaches the threshold, the link is taken out of service.
MTP2AERM	Status of the alignment error rate monitor state machine (AERM).	IDLE—State machine is inactive. MONITORING—Alignment error monitor is active. This is part of the alignment process.
MTP2CONGESTION	Status of the congestion control state machine.	IDLE—State machine is inactive. No congestion is detected; normal traffic flow. ACTIVE—Congestion has been declared. The Cisco 2600 series router is sending SIBs every T5, which indicates that the remote end should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Congestion Backhaul	Congestion status of the backhaul link between the Cisco SLT and the media gateway controller.	Abate—Link between the Cisco 2600 series router and the media gateway controller is not under congestion. Onset—Link between the Cisco 2600 series router and the media gateway controller is under congestion. and the Media Gateway Controller should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Remote Processor Outage	Processor outage status of the remote.	TRUE indicates that the remote is in processor outage. FALSE indicates that the remote has not declared processor outage.
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE—Indicates that forced retransmission is enabled. FALSE—Indicates that forced retransmission is disabled.
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE—Indicates that PCR is enabled. FALSE—Indicates that PCR is disabled.
N2	Status of the N2 parameter.	Octet counts are specified.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.

show ss7 mtp2 stats

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) operational statistics, use the **show ss7 mtp2 stats** command in privileged EXEC mode.

show ss7 mtp2 stats [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default Information for all channels is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples The following is sample output from this command showing operations and maintenance (OM) statistics for MTP2 channel 0:

```
Router# show ss7 mtp2 stats 0

SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0

OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0

OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0

OMLSSU_XMIT_Count       = 17
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 0
OMLSSU_XMIT_SIOSCount   = 17
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0

OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
OMLSSU_RCV_SIECount     = 0
OMLSSU_RCV_SIOCount     = 0
```

```
OMLSSU_RCV_SIOSCount     = 0
OMLSSU_RCV_SIPOCount     = 0
OMLSSU_RCV_SIBCount      = 0
OMLSSU_RCV_InvalidCount  = 0

OMRemote_PO_Count        = 0
OMRemote_Congestion_Cnt  = 0

OMtimeINSV (secs)        = 0
OMtimeNotINSV (secs)     = 9550
OMMSUBytesTransmitted    = 0
OMMSUBytesReceived       = 0

OMTransmitReqCount       = 33
OMPDU_notAcceptedCount   = 0
OMPDU_NACK_Count         = 0
OMunreasonableFSN_rcvd   = 0
OMunreasonableBSN_rcvd   = 0

OMT1_TMO_Count           = 0
OMT2_TMO_Count           = 0
OMT3_TMO_Count           = 0
OMT4_TMO_Count           = 0
OMT5_TMO_Count           = 0
OMT6_TMO_Count           = 0
OMT7_TMO_Count           = 0
OMT8_TMO_Count           = 0
OMTA_TMO_Count           = 0
OMTF_TMO_Count           = 0
OMTO_TMO_Count           = 0
OMTS_TMO_Count           = 477218
OMLostTimerCount         = 0

OMOMLostBackHaulMsgs     = 0

OMAERMCount              = 0
OMAERMFailCount          = 0
OMSUERMCount             = 0
OMSUERMFailCount         = 0
OMCongestionCount        = 0
OMCongestionBackhaulCnt  = 0
```

Table 175 describes significant fields shown in this output.

Table 175 show ss7 mtp2 stats Field Descriptions

Field	Description
OMIACAlignAttemptCount OMIACAlignFailCount OMIACAlignCompleteCount	Counts for Initial Alignment Control (IAC) attempts.
OMMSU_TO_XMIT_Count	Related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. The number shown in OMMSU_TO_XMIT_Count is less than the PDU_pkts_recieve_count because OMMSU_TO_XMIT_Count shows the number of PDUs going out on the link, while the PDU_pkts_recieve_count includes PDUs that are internal to MTP2.
OMMSU_RCV_Count	Related to the results of the **show ss7 sm stats** command's packets_send_count.

Table 175 show ss7 mtp2 stats Field Descriptions (continued)

Field	Description
OMLSSU_XMIT_Count OMLSSU_XMIT_SINCount OMLSSU_XMIT_SIECount OMLSSU_XMIT_SIOCount OMLSSU_XMIT_SIOSCount OMLSSU_XMIT_SIPOCount OMLSSU_XMIT_SIBCount	Number of times that MTP 2 has posted the specific Link Status Signal Unit (LSSU) to MTP 1. They do not show the number of LSSUs actually sent over the link.
OMLSSU_RCV_Count OMLSSU_RCV_SINCount OMLSSU_RCV_SIECount OMLSSU_RCV_SIOCount OMLSSU_RCV_SIOSCount OMLSSU_RCV_SIPOCount OMLSSU_RCV_SIBCount OMLSSU_RCV_InvalidCount	Number of LSSUs received by MTP 2 from MTP 1. Because of MTP 1 filtering, this is not the same as the actual LSSUs sent over the link.
OMT1_TMO_Count OMT2_TMO_Count OMT3_TMO_Count OMT4_TMO_Count OMT5_TMO_Count OMT6_TMO_Count OMT7_TMO_Count OMT8_TMO_Count OMTA_TMO_Count OMTF_TMO_Count OMTO_TMO_Count OMTA_TMO_Count OMLostTimerCount	Information about timers in use.
OMLostBackhaulMsgs	How many messages received from the Media Gateway Controller have been lost because of a lack of resources in the Cisco 2600 series router. This count is related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. For example, if the Media Gateway Controller sends 100 MSUs and the Cisco 2600 series router only has 65 free buffers, 35 MSUs might be lost.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 timer	Displays durations of the SS7 MTP2 state-machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 timer

To display durations of the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine timers, use the **show ss7 mtp2 timer** command in privileged EXEC mode.

show ss7 mtp2 timer [*channel*]

Note The eight timers whose status is displayed using this command are set on the media gateway controller using MML commands. The timers are then downloaded from the controller to the Cisco signaling link terminal (SLT).

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default Information for all sessions is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines MTP2 uses eight different timers on each link. Throughout the link-state transitions, multiple timers are active. An in-service MTP2 link requires timers that are constantly started, stopped, and restarted. Use this command to display the configured timer durations.

Note All MTP2 configuration parameters are set at the Cisco SLT command-line interface. Media gateway controller parameter data files are no longer used to configure the Cisco SLT.

Examples The following is sample output from this command displaying timer information for channel 0:

```
Router# show ss7 mtp2 timer 0

SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
    T1 aligned/ready = 15000
      T2 not aligned = 5000
          T3 aligned = 3000
T4 Emergency Proving = 3000
   T4 Normal Proving = 3000
      T5 sending SIB = 200
      T6 remote cong = 3000
 T7 excess ack delay = 2000
```

```
  T8 errored int mon = 0
TA SIE timer = 20
       TF FISU timer = 20
        TO SIO timer = 20
       TS SIOS timer = 20
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 stats	Displays SS7 MTP2 operational statistics.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 variant

To display information about the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) protocol variant, use the **show ss7 mtp2 variant** command in privileged EXEC mode.

show ss7 mtp2 variant [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5350 and Cisco AS5400.

Usage Guidelines

This command can take an optional channel ID at the end (for example, **show ss7 mtp2 variant 0**). If the optional channel ID is omitted, the command displays the SS7 variant for all configured SS7 links.

Each country specifies its own variant of SS7, and the Cisco SLT supports several variants of the MTP2 protocol. The selected variant can affect the MTP2 statistics displayed by various commands. The Cisco SLT support the following variants:

- Telcordia Technologies (formerly Bellcore)
- ITU: International Telecommunication Union
- NTT: Japanese Nippon Telephone and Telegraph Cellular System
- TTC: Japanese Telecommunications Technology Committee

Each channel can be configured to any one of the protocol variants. When you change from one variant to another, for example from Bellcore to NTT, the MTP2 parameters default to those specified by NTT. You can then change the defaults as required.

Examples

The following is sample output from this command showing protocol-variant information for channel 1:

```
Router# show ss7 mtp2 variant 1

Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for the SS7 link whose channel ID is 2:

```
Router# show ss7 mtp2 variant 2
```

```
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for all configured links:

```
Router# show ss7 mtp2 variant

Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 3 is Bellcore GR-246-Core Issue 2, Dec 1997
```

Field descriptions should be self-explanatory. Note, however, the following:

- In each case, all SS7 links are clearly provisioned to use the Bellcore variant (see the **ss7 mtp2 variant bellcore** command).
- Command output shows that the MTP2 variant is being used for each of the SS7 links and that the Telcordia Technologies (formerly Bellcore) version is implemented; it also shows where the links are identified by their assigned channel IDs.

Related Commands

Command	Description
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 channel-id	Displays information for a given session channel ID.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
ss7 mtp2 variant bellcore	Configures the device for Telcordia Technologies (formerly Bellcore) standards.

show ss7 sm session

To display information about a Signaling System 7 (SS7) Session Manager session, use the **show ss7 sm session** command in privileged EXEC mode.

show ss7 sm session [*session*]

Syntax Description

session	(Optional) Session. Range is from 0 to 3.

Command Default Information for all sessions is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for up to four Session Manager sessions was added.

Usage Guidelines If no sessions are configured, the message "No Session is configured" appears.

Support for up to four Session Manager sessions was added in Cisco IOS Release 12.2(11)T. Session Manager sessions are now numbered from 0 to 3. The *Cisco Signalling Link Terminal Dual Ethernet* feature changes the command-line-interface syntax and adds sessions 2 and 3.

Examples The following is sample output from this command displaying session information for both sessions:

```
Router# show ss7 sm session

Session[0]: Remote Host 255.255.251.254:8060, Local Host 255.255.255.254:8060
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32

Session[1]: Remote Host 255.255.251.255:8061, Local Host 255.255.255.254:8061
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
```

Table 176 describes significant fields shown in this output.

Table 176 show ss7 sm session Field Descriptions

Field	Description
Remote Host, Local Host	IP address and port number for the session.
retrans_t	Retransmission timer value.
cumack_t	Cumulative acknowledgment timer value.
m_cumack	Maximum number of segments that can be received before the RUDP sends an acknowledgment.
m_outseq	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
m_rcvnum	Maximum number of segments that the remote end can send before receiving an acknowledgment.

Related Commands

Command	Description
ss7 session	Establishes a session.
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.

show ss7 sm set

To display information about the Signaling System 7 (SS7) session set state, failover timer, member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets, use the **show ss7 sm set** command in privileged EXEC mode.

show ss7 sm set [*ss-id-range*]

Syntax Description

ss-id-range	(Optional) Displays the SS7 session set ID, state, member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(15)T	The *ss-id-range* argument was added. This command previously displayed only the failover-timer value and had no arguments.

Usage Guidelines

This command is available on all Cisco Signaling Link Terminal (SLT) platforms.

If the optional *ss-id-range* argument is omitted, information is displayed for all SS7 session sets. The following are valid SS7 session set ranges. The default is 3 seconds.

1	Selects SS7 session set 1.
0, 2, 3	Selects SS7 session sets 0, 2, and 3.
0-2	Selects SS7 session sets 0, 1, and 2.
0, 2-3	Selects SS7 session sets 0, 2, and 3.
0, 2	Selects SS7 session sets 0 and 2.

Examples

The following is sample output from this command displaying failover timer information; the failover timer is set to the default of 3 seconds:

```
Router# show ss7 sm set

Session Manager Set
      failover timer = 3 seconds
```

The following example displays the SS7 session set state, failover-timer, member sessions, and SS7 links that belong to a range of SS7 session sets:

```
Router# show ss7 sm set

Session-set:0
  State          = ACTIVE
```

```
  Failover-timer = 5 secs.
  2 Sessions:
    session 0  session-state ACTIVE   remote-host 172.16.0.0:5555
    session 1  session-state STANDBY  remote-host 172.31.255.255:4444
  3 SS7 Links:
       7/0 (ser.)    chan-id 0  variant Bellcore   link-state INSERVICE
       7/0:0 (dig.)  chan-id 1  variant Bellcore   link-state INSERVICE
       7/0:2 (dig.)  chan-id 3  variant Bellcore   link-state INITIAL_ALIGNMENT
Session-set:1
  State          = IDLE
  Failover-timer = 5 secs.
  0 Sessions:
  0 SS7 Links:
Session-set:2
  State          = ACTIVE
  Failover-timer = 5 secs.
  2 Sessions:
    session 2  session-state ACTIVE   remote-host 172.16.0.0:6666
    session 3  session-state STANDBY  remote-host 172.31.255.255:7777
  1 SS7 Links:
       7/0:1 (dig.)  chan-id 2  variant Bellcore   link-state INSERVICE
Session-set:3
  State          = IDLE
  Failover-timer = 5 secs.
0 Sessions:
  0 SS7 Links:
```

Table 177 describes significant fields in this output.

Table 177 show ss7 sm set Field Descriptions

Field	Description
Session-set:0	One of four SS7 session sets is configured.
State	The session is ACTIVE.
Failover-timer	`The number of seconds is set to 5.`
2 Sessions:	• Session 0—session state is ACTIVE and connected to port 5555 of remote-host 172.16.0.0 • Session 1—session state is STANDBY and connected to port 4444 of remote-host 172.31.255.255
3 SS7 Links:	• SS7 link at serial interface 7/0 has channel ID 0 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:0 has channel ID 1 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:2 has channel ID 3 and current MTP2 link state of INITIAL_ALIGNMENT.
Session-set:1	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.
Session-set:2	One of four SS7 session sets is configured.
State	The session is ACTIVE.

Table 177 show ss7 sm set Field Descriptions (continued)

Field	Description
Failover-timer	`The number is set to 5 seconds.`
2 Sessions:	• Session 2 is ACTIVE and connected to port 6666 of remote host 172.16.0.0 • Session 3 is STANDBY and connected to port 7777 of remote host 172.31.255.255.
1 SS7 Links:	SS7 link at serial interface 7/0:1 has channel ID 2 and current MTP2 link state of INSERVICE.
Session-set:3	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set	Independently selects failover-timer values for each session set and specifies the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

show ss7 sm stats

To display Signaling System 7 (SS7) Session Manager session statistics, use the **show ss7 sm stats** command in privileged EXEC mode.

show ss7 sm stats

Syntax Description There are no arguments or keywords for this command.

Command Default The command shows information for both sessions.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines If no sessions are configured, the message "No Session is configured" appears.

Examples The following is sample output from this command displaying SS7 Session Manager statistics. The fields are self-explanatory and show information about the session state, protocol data units (PDUs) packets sent and received, and SS7 Reliable User Datagram Protocol (RUDP) performance:

```
Router# show ss7 sm stats

-------------------- Session Manager  --------------------

Session Manager state              = SESSION SET STATE-ACTIVE
Session Manager Up count           = 1
Session Manager Down count         = 0
   lost control packet count       = 0
              lost PDU count       = 0
 failover timer expire count       = 0
 invalid_connection_id_count       = 0

Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count                = 0
   Open Retry count               = 0

   Total Pkts receive count       = 1
   Active Pkts receive count      = 0
   Standby Pkts receive count     = 1
   PDU Pkts receive count         = 0
   Unknown Pkts receive count     = 0

Pkts send count                 = 0
   Pkts requeue count             = 0
    -Pkts window full count       = 0
```

```
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0

   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0

Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count               = 0
   Open Retry count              = 0

   Total Pkts receive count      = 2440
   Active Pkts receive count     = 1
   Standby Pkts receive count    = 0
   PDU Pkts receive count        = 2439
   Unknown Pkts receive count    = 0

   Pkts send count               = 2905
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0

   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear ss7 sm-stats	Clears the counters that track Session Manager statistics for the **show ss7 sm stats** command.
ss7 session	Establishes a session.

show stcapp buffer-history

To display event logs for SCCP Telephony Control Application (STCAPP) analog voice ports, use the **show stcapp buffer-history** command in privileged EXEC mode.

show stcapp buffer-history {**all** | **port** *port*}

Syntax Description

all	Displays event records for all analog voice ports.
port *port*	Displays event records for only the specified analog voice port. **Note** *Port* syntax is platform-dependent; type ? to determine.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

To display event logs with this command, you must first enable event logging using the **debug voip application stcapp buffer-history** command.

Note Using the **all** keyword with this command could increase CPU utilization by as much as 40%.

Examples

The following is sample output from the **show sctapp buffer-history** command showing voice port 2/3 registering with the call-control system, going offhook, and then disconnecting:

```
Router# show stcapp buffer-history port 2/3

1. [2/3], 00:00:44.467
IS [DEVICE_UNREGISTERING] --> IS
2. [2/3], 00:00:44.467
IS [DEVICE_RESETTING] --> OOS
3. [2/3], 00:00:44.467
OOS [DEVICE_DESTROYED] --> STATE_NONE
4. [2/3], 00:00:46.455
STATE_NONE [DEVICE_CREATED] --> OOS
5. [2/3], 00:00:46.455
OOS [DEVICE_REGISTERING] --> INIT
6. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_REGISTER_DONE] --> INIT
7. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_CAP_REQ] --> INIT
8. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_BUTTON_TEMP_RES] --> INIT
9. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_FORWARD_STAT_RES] --> INIT
10. [2/3], 00:00:47.151
INIT [STCAPP_DC_EV_DEVICE_LINE_STAT_RES] --> INIT
11. [2/3], 00:00:47.163
```

```
INIT [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> INIT
12. [2/3], 00:00:47.419
IS [STCAPP_DC_EV_DEVICE_DEFINE_DATE_TIME_RES] --> IS
13. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
14. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
15. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
16. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
17. [2/3], 00:06:00.923
IDLE [STCAPP_CC_EV_CALL_SETUP_IND] --> OFFHOOK
18. [2/3], 00:06:01.019
OFFHOOK [STCAPP_DC_EV_DEVICE_CALL_STATE_OFFHOOK (245)] --> OFFHOOK
19. [2/3], 00:06:01.023
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
20. [2/3], 00:06:01.023
OFFHOOK [STCAPP_DC_EV_DEVICE_START_TONE (245)] --> OFFHOOK
21. [2/3], 00:06:01.023
OFFHOOK [STCAPP_CC_EV_CALL_REPORT_DIGITS_DONE] --> OFFHOOK
22. [2/3], 00:06:03.083
OFFHOOK [STCAPP_CC_EV_CALL_DISCONNECTED] --> ONHOOK_DISCONNECT
23. [2/3], 00:06:03.295
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
24. [2/3], 00:06:03.295
ONHOOK_DISCONNECT [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK (245)] --> IDLE
25. [2/3], 00:06:03.299
IDLE [STCAPP_DC_EV_DEVICE_STOP_TONE (245)] --> IDLE
26. [2/3], 00:06:03.303
IDLE [STCAPP_CC_EV_CALL_DISCONNECT_DONE] --> IDLE
```

Related Commands

Command	Description
debug voip application stcapp buffer-history	Enables event logging for STCAPP analog voice ports.
show stcapp statistics	Displays call statistics for STCAPP analog voice ports.

show stcapp device

To display configuration information about Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) analog voice ports, use the **show stcapp device** command in privileged EXEC mode.

show stcapp device {**name** *device-name* | **summary** | **voice-port** *port*}

Syntax Description

name *device-name*	Displays information for the analog voice port with the specified device name. The device name is the unique device ID that is assigned to the port when it registers with the call-control system.
summary	Displays a summary of all voice ports.
voice-port *port*	Displays information for the specified analog voice port. **Note** The *port* syntax is platform-dependent; type ? to determine appropriate port numbering.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was modified. Command output was enhanced to display call control block (CCB) and call-control device information.
12.4(4)T	This command was modified. Command output was enhanced to display supported modem transport capability.
12.4(6)XE	This command was modified. Command output was enhanced to display visual message waiting indicator (VMWI) and information for Dial Tone After Remote Onhook feature.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. Command output was enhanced to display the call waiting tone configuration.

Usage Guidelines

Use this command to display configuration and voice interface card (VIC)-specific port information. The Active Call Info field is populated only if a call is active on the voice port.

Examples

The following is a sample output showing IPv6 addresses for the local and remote sites:

```
Router# show stcapp device voice-port 2/0

Port Identifier: 2/0
Device Type: ALG
Device Id: 1
Device Name: AN1AE2853624400
Device Security Mode : None
Modem Capability: None
Device State: IS
Diagnostic: None
Directory Number: 1000
Dial Peer(s): 1000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event: STCAPP_DC_EV_DEVICE_CALL_INFO
Line State: ACTIVE
Hook State: OFFHOOK
mwi: DISABLE
vmwi: OFF
PLAR: DISABLE
Number of CCBs: 1
Global call info:
Total CCB count = 2
Total call leg count = 4

Call State for Connection 1: TsConnected
Connected Call Info:
Call Reference: 22690511
Local IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Local IP Port: 17424
Remote IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Remote IP Port: 18282
Calling Number: 1000
Called Number:
Codec: g729br8
SRTP: off
```

The following is a sample output from the **show stcapp device** command for an SCCP analog port with VMWI while the Dial Tone After Remote Onhook Feature is activated:

```
Router# show stcapp device voice-port 2/4
Port Identifier:  2/4
Device Type:      ALG
Device Id:        4
Device Name:      AN0C863967C9404
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 7204
Dial Peer(s):     4
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              ENABLE
vmwi:             ON
PLAR:             DISABLE
Number of CCBs:   0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port on a VIC2-2FXS voice interface card specified by the port number:

```
Router# show stcapp device voice-port 1/0/0

Port Identifier:  1/0/0
Device Type:      ALG
Device Id:        3
Device Name:      AN1EBEEB6070200
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2099
Dial Peer(s):     999100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
ccw_on:           FALSE
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Callback State:   DISABLED
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C863972F5401

Port Identifier:  2/1
Device Type:      ALG
Device Id:        25
Device Name:      AN0C863972F5401
Device State:     IS
Diagnostic:       None
Directory Number: 9101
Dial Peer(s):     2
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Hook State:       OFFHOOK
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 1: TsConnected
Connected Call Info:
   Call Reference: 16777509
   Local IP Addr:  10.1.0.1
   Local IP Port:  18768
   Remote IP Addr: 10.1.0.1
   Remote IP Port: 18542
   Calling Number: 9101
   Called Number:  9102
   Codec:          g711ulaw
```

The following is a sample output from the **show stcapp device** command for STCAPP analog voice ports:

```
Router# show stcapp device summary

Total Devices:           24
Total Calls in Progress: 3
Total Call Legs in Use:  6

Port       Device          Device   Call          Dev  Directory   Dev
Identifier Name            State    State         Type Number      Cntl
---------- --------------- -------- ------------- ---- ----------- ----
2/1        AN0C863972F5401 IS       ACTIVE         ALG  9101       CCM
2/2        AN0C863972F5402 IS       ACTIVE         ALG  9102       CCM
2/3        AN0C863972F5403 IS       ACTIVE         ALG  9103       CCM
2/0        AN0C863972F5400 IS       IDLE           ALG  9100       CCM
2/4        AN0C863972F5404 IS       IDLE           ALG  9104       CCM
2/5        AN0C863972F5405 IS       IDLE           ALG  9105       CCM
2/6        AN0C863972F5406 IS       IDLE           ALG  9106       CCM
2/7        AN0C863972F5407 IS       IDLE           ALG  9107       CCM
2/8        AN0C863972F5408 IS       IDLE           ALG  9108       CCM
2/9        AN0C863972F5409 IS       IDLE           ALG  9109       CCM
2/10       AN0C863972F540A IS       IDLE           ALG  9110       CCM
2/11       AN0C863972F540B IS       IDLE           ALG  9111       CCM
2/12       AN0C863972F540C IS       IDLE           ALG  9112       CCM
2/13       AN0C863972F540D IS       IDLE           ALG  9113       CCM
2/14       AN0C863972F540E IS       IDLE           ALG  9114       CCM
2/15       AN0C863972F540F IS       IDLE           ALG  9115       CCM
2/16       AN0C863972F5410 IS       IDLE           ALG  9116       CCM
2/17       AN0C863972F5411 IS       IDLE           ALG  9117       CCM
2/18       AN0C863972F5412 IS       IDLE           ALG  9118       CCM
2/19       AN0C863972F5413 IS       IDLE           ALG  9119       CCM
2/20       AN0C863972F5414 IS       IDLE           ALG  9120       CCM
2/21       AN0C863972F5415 IS       IDLE           ALG  9121       CCM
2/22       AN0C863972F5416 IS       IDLE           ALG  9122       CCM
2/23       AN0C863972F5417 IS       IDLE           ALG  9123       CCM
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C86385E3D400

Port Identifier: 2/0
Device Type:      ALG
Device Id:        1
Device Name:      AN0C86385E3D400
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2400
Dial Peer(s):     2000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
PLAR:             DISABLE
Callback State:   IDLE
```

```
CWT Repetition Interval: 0 second(s)
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

Table 178 describes the significant fields shown in these displays, in alphabetical order.

Table 178 show stcapp device Field Descriptions

Field	Description
Active Call Info	Displays only when an active call is in progress.
Call Reference	Reference number created by Cisco Unified Communications Manager to track messages associated with a specific call.
Call State	Call processing state: • ACTIVE—Established call connection • IDLE—No call connection • UNREGISTERED—Device is not registered with the Cisco Unified Communications Manager
Called Number	Device called number.
Calling Number	Device calling number.
ccw_on	Displays status of Cancel Call Waiting feature: • False—Inactive on port. • True—Active on port.
Codec	Displays codec type.
CWT Repetition Interval	Displays the call waiting tone configuration.
Dev Cntl	Call-control device that is managing the analog endpoints. CCM represents Cisco Unified Communications Manager. CME represents Cisco Unified Communications Manager Express.
Device Id	Identifier used between the Cisco Unified Communications Manager and gateway to uniquely identify an endpoint.
Device Name	Unique device ID of the analog endpoint. The device ID is derived from an algorithm using the MAC address of the SCCP interface on the voice gateway and the hexadecimal translation of the port's slot number and port number.

Table 178 show stcapp device Field Descriptions (continued)

Field	Description
Device State	Displays whether device is available for use: • ACTIVE_PENDING—Call is pending certain events before going active. • INFO_RCVD—Call information is received from the Cisco Unified Communications Manager during call setup. • INIT—Waiting to reinitialize. • IS—In service. • OFFHOOK—Device is off-hook. • OFFHOOK_TIMEOUT—Digit timeout occurred while the device is off-hook. • ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • OOS—Out of service. • PROCEED—Dialed number translation is complete and call setup is in progress. • REM_ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • RINGING—An incoming call has invoked ringing of the receiving device.
Device Type	Shows phone type: • ALG—Analog. • BRI—ISDN BRI.
Diagnostic	Reason code for a device error condition.
Dial Peer(s)	Dial peer name.
Dialtone after remote onhook feature	Displays feature status: • Activated • Not activated
Directory Number	Assigned to the device by the Cisco Unified Communications Manager.
Last Event	Last event processed by this port.
Local IP Addr	IPv4 address of this gateway used to stream audio using the Real-Time Transport Protocol (RTP).
Local IPv6 Addr	IPv6 address of this gateway used to stream audio using the RTP.
Local IP Port	IP port of this gateway used to stream audio using RTP.
Port Identifier	Identifies the physical voice port.
Remote IP Addr	IPv4 address of the far-end gateway that streams audio using RTP.
Remote IPv6 Addr	IPv6 address of the far-end gateway that streams audio using RTP.

Table 178 show stcapp device Field Descriptions (continued)

Field	Description
Remote IP Port	IP port of the far-end gateway that streams audio using RTP.
vmwi	Displays LED status: • On • Off

Related Commands

Command	Description
show stcapp statistics	Displays call statistics for STCAPP devices.

show stcapp feature codes

To display current values for feature access codes (FACs), feature speed-dials (FSDs), and feature callback in the SCCP telephony control (STC) application, use the **show stcapp feature codes** command in privileged EXEC mode.

show stcapp feature codes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	This command was modified. Speed-dial output was expanded to include number of digits.
12.4(6)XE	This command was modified. This command was enhanced to display standard and feature call-control modes.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(20)YA	This command was modified. Command output was enhanced to include values for callback and meetme-conference.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command shows all values for the following in standard and feature mode, depending on the configuration on the Cisco IOS gateway:

- feature access codes (FACs)
- feature speed-dials (FSD)
- feature callback in the STC application

You can enable FACs and FSDs by using the **stcapp feature access-code** and **stcapp feature speed-dial** commands.

You can enable callback by using the **stcapp feature callback** command.

Examples

The following example displays the values for STC application feature codes if FACs and FSDs are not enabled:

```
Router# show stcapp feature codes

  stcapp feature access-code disabled
  stcapp feature speed-dials disabled
```

```
 stxcapp call-control mode is standard
```

The following example shows that feature mode for call-control is enabled:

```
Router# show stcapp feature codes

  stcapp feature speex-dial disabled
  stacapp call-control mode is feature mode
    #1 -- hangup last active call
    #2 - transfer
    #3 - conference
    #4 -- drop last conferee
    #5 -- toggle between two calls
```

The following example displays the default values for all STC application feature codes, including CallBack on Busy and SCCP Meet-Me Conference:

```
Router# show stcapp feature codes

  stcapp feature access-code
    malicious call ID (MCID) ***
    prefix **
    call forward all **1
    call forward cancel **2
    pickup local group **3
    pickup different group **4
    meetme-conference **5
    pickup direct **6
    cancel call waiting **8

  stcapp feature speed-dial
    prefix *
    redial *#
    speeddial number of digit(s) 1
    voicemail *0
    speeddial1 *1
    speeddial2 *2
    speeddial3 *3
    speeddial4 *4
    speeddial5 *5
    speeddial6 *6
    speeddial7 *7
    speeddial8 *8
    speeddial9 *9

  stcapp feature callback
    key #1
    timeout 30
```

Table 179 describes significant fields shown in the output of this command, in alphabetical order.

Table 179 show stcapp feature codes Field Descriptions

Field	Description
call forward all	FAC prefix plus FAC set by the **call forward all** command.
call forward cancel	FAC prefix plus FAC set by the **call forward cancel** command.
cancel call waiting	FAC prefix plus FAC set by the **cancel-call-waiting** command.
key	Code set for call back on Busy by the **activation-key** command.
meetme-conference	FAC prefix plus FAC set by the **meetme-conference** command.
pickup different group	FAC prefix plus FAC set by the **pickup group** command.

Table 179 show stcapp feature codes Field Descriptions (continued)

Field	Description
pickup direct	FAC prefix plus FAC set by the **pickup direct** command.
pickup local group	FAC prefix plus FAC set by the **pickup local** command.
prefix	FAC prefix set by the **prefix** (stcapp-fsd) command or by the **prefix (stcapp-fac)** command.
redial	FSD prefix plus FSD code set by the **redial** command.
speeddial number of digit(s)	FSD digit length set by the **digit** command.
speeddial*x*	FSD prefix plus FSD code from the range set by the **speed dial** command.
timeout	Period in seconds for ringing timer set for Call back on Busy by using the **ringing-timeout** command.
voicemail	FSD prefix plus FSD code set by the **voicemail** command.

Related Commands

Command	Description
activation-key	Defines the activation key for Callback on Busy.
call forward all	Designates an STC application feature access code to activate the forwarding of all calls.
call forward cancel	Designates an STC application feature access code to cancel the forwarding of all calls.
digit	Designates the number of digits for STC application feature speed-dial codes.
meetme-conference	Designates an STC application feature access code for meetme-conference.
pickup direct	Designates an STC application feature access code for directed call pickup.
pickup group	Designates an STC application feature access code for group call pickup from another group.
pickup local	Designates an STC application feature access code for group call pickup from the local group.
prefix (stcapp-fac)	Designates a prefix to precede the dialing of an STC application feature access code.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
ringing-timeout	Defines ringing timer for Callback on Busy.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature callback	Enables CallBack on Busy and enters the STC application feature callback configuration mode
stcapp feature access-code	Enters STC application feature access code configuration mode to set feature access codes.

Command	Description
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

show stcapp statistics

To display call statistics for SCCP Telephony Control Application (STCAPP) voice ports, use the **show stcapp statistics** command in privileged EXEC mode.

show sctapp statistics [**all** | **voice-port** *port-number*]

Syntax Description

voice-port *port-number*	(Optional) Displays information for a specific voice port. • *port-number*—Number of the port on the interface. Refer to the appropriate platform manual or online help for port numbers on your networking device.
all	(Optional) Displays a summary of all voice ports.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to display call statistics for STCAPP voice ports.

Examples

The following is sample output for the **show sctapp statistics** command for STCAPP voice port 1/0/0.1:

```
Router# show stcapp statistics voice-port 1/0/0.1

STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
---------- -------- -------- -------- -------- --------
1/0/0.1 0        7        0        0        0
```

The following is sample output for the **show stcapp statistics** command for all STCAPP voice ports:

```
Router# show stcapp statistics all

STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
---------- -------- -------- -------- -------- --------
1/0/0            0        7        0        0        0
1/0/1            0        0        7        0        0
1/0/3            0        0        0        0        0
1/1/0.1          0        0        0        0        0
1/1/1.1          0        0        0        0        0
1/0/2            0        0        0        0        0
```

Table 180 describes the significant fields shown in the display.

Table 180 show stcapp statistics Field Descriptions

Field	Description
DevErr	Device errors.
CallOA	Call origination attempts.
CallTA	Call termination attempts.
CallErr	Call errors.
CallPE	Call preemptions.

Related Commands

Command	Description
show stcapp device	Displays configuration information about STCAPP voice port.s

show subscription

To display information about Application Subscribe/Notify Layer (ASNL)-based and non-ASNL-based SIP subscriptions, use the **show subscription** command in user EXEC or privileged EXEC mode.

show subscription {**asnl session** {**active** | **history** [**errors** | **session-id** *session-id* | **url**] | **statistics**} | **sip**} [**summary**]

Syntax Description

asnl session	ASNL-based subscriptions.
active	Active subscriptions
history	ASNL history table in detailed format.
errors	(Optional) Subscription or notification errors available in the history table.
session-id *session-id*	(Optional) Details of subscriptions matched by session id.
url	(Optional) ASNL subscriptions on a per-URL basis.
statistics	ASNL-based subscriptions.
sip	Both ASNL and non-ASNL based subscriptions.
summary	(Optional) ASNL history table in compact format.

Command Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to specify options for displaying ASNL and SIP subscription information. If you have a TCL application that uses the SUBSCRIBE and NOTIFY for External Triggers feature, you can use either the **show subscription sip** or **show subscription asnl** command to display subscription information. However, the **asnl** keyword provides more display options.

Examples

The following examples show ASNL-based active subscriptions. The first example displays the information in detail. The second example displays the information in summary form:

```
Router# show subscription asnl session active

ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions: 1
URL: sip:user@10.7.104.88
  Event Name : stress
  Session ID : 8
  Expiration Time : 50 seconds
```

```
  Subscription Duration : 5 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received  : 2
  Last response code : ASNL_NOTIFY_RCVD
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:17 UTC Apr 9 2000
  Application that subscribed : stress
  Application receiving notification: stress

Router# show subscription asnl session active summary

ASNL Active Subscription Records Summary:
 ========================================
Number of active subscriptions: 104
SubId      CallId     Proto          URL                              Event
-----      ------     -----          ---                              -----
14090      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88              newstress
14091      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88              newstress
14092      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88              newstress
14093      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88              newstress
14094      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88              newstress

Subscription HISTORY command (detailed display)

Router# show subscription asnl session history

ASNL Subscription History Records Details:
==========================================
Total history records                          = 1
Total error count                              = 0
Total subscription requests sent               = 1
Total subscription requests received           = 0
Total notification requests sent               = 0
Total notification requests received           = 3
URL: sip:user@10.7.104.88
  Event Name : stress
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 10 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received : 3
  Last response code : ASNL_UNSUBSCRIBE_SUCCESS
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:22 UTC Apr 9 2000

Subscription HISTORY (Summary display)
```

```
Router# show subscription asnl session history summary

ASNL Subscription History Records Summary:
==========================================
Total history records = 2
Total error count = 0
Total subscription requests sent = 2
Total subscription requests received = 0
Total notification requests sent = 0
Total notification requests received = 6

URL                                                 Session ID  Call ID
---                                                 ----------  -------
sip:user@10.7.104.88                                     9           5
sip:user@10.7.104.88                                     8           5
```

Table 181 describes significant fields in the displays.

Table 181 show subscription Field Descriptions

Field	Description
Last response code	ASNL response codes: ASNL_NONE—Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS—Subscription request was successful. ASNL_SUBSCRIBE_PENDING—Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED—Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR—Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR—Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED—Subscription expired. ASNL_SUBSCRIBE_CLEANUP—Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS—Subscription termination request was successful.

Table 181 show subscription Field Descriptions

Field	Description
Last response code (continued)	ASNL_UNSUBSCRIBE_PENDING—Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED —Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR—Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD—Received a notification request from the subscription server.
Last error code	Subscription error codes: ASNL_SUBSCRIBE_PENDING—Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED—Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR—DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR—Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED—Subscription expired.

Table 181 show subscription Field Descriptions

Field	Description
Last error code (continued)	ASNL_UNSUBSCRIBE_FAILED —Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR—Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription termination request from the client.

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
subscription asnl session history	Specifies how long to keep ASNL subscription history records and how many history records to keep in memory.
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

show subscription local

To show all the LOCAL Subscribe/Notify Service Provider (SNSP) subscriptions, use the **show subscription local** command in privileged EXEC mode.

show subscription local [**aaa**] [**summary**]

Syntax Description

aaa	(Optional) Subscriptions for voice authentication, authorization, and accounting (AAA) server applications under local SNSP.
summary	(Optional) Summary of all subscriptions.

Command Default All LOCAL SNSP subscriptions are displayed in detailed format.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Use this command to display all the subscriptions for voice AAA server applications under LOCAL SNSP in a detailed or summary format.

Examples The following is sample output from the **show subscription local** command:

```
Router# show subscription local

ASNL Active Subscription Records Details:
=========================================

Number of active subscriptions:2


URL:local://aaa
  Event Name                 :accounting-notification
  Session ID                 :1
  Expiration Time            :5000 seconds
  Subscription Duration      :0 seconds
  Protocol                   :ASNL_PROTO_LOCAL
  Call ID                    :N/A
  Total Subscriptions Sent   :1
  Total Notifications Received:1
  Last response code         :ASNL_NOTIFY_RCVD
  Last error code            :ASNL_NONE
  First Subscription Time    :00:48:12 UTC Dec 18 2002
  Last Subscription Time     :00:48:12 UTC Dec 18 2002
  First Notify Time          :00:48:12 UTC Dec 18 2002
  Last Notify Time           :00:48:12 UTC Dec 18 2002
```

```
  Application that subscribed       :GAS
  Application receiving notification:N/A
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :0 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :1
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:48:12 UTC Dec 18 2002

  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :no
```

The following is sample output from the **show subscription local aaa** command:

```
Router# show subscription local aaa

ASNL Active Subscription Records Details:
=========================================

Number of active subscriptions:2


URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :140 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :2
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:50:32 UTC Dec 18 2002

  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :yes
```

Table 182 describes significant fields shown in the displays.

Table 182 show subscription local aaa Field Descriptions

Field	Description
Last response code	ASNL response codes. The field can be one of the following values: ASNL_NONE—Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS—Subscription request was successful. ASNL_SUBSCRIBE_PENDING—Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED—Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR—Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR—Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED—Subscription expired. ASNL_SUBSCRIBE_CLEANUP—Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS—Subscription termination request was successful. ASNL_UNSUBSCRIBE_PENDING—Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED —Subscription termination request failed.

Table 182 show subscription local aaa Field Descriptions (continued)

Field	Description
Last response code (continued)	ASNL_UNSUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR—Subscriptio n termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR—Atte mpt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR—Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD—Received a notification request from the subscription server.
Last error code	Subscription error codes. The field can be one of the following values: ASNL_SUBSCRIBE_PENDING—Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED—Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR—Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR—DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR—Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR—Internal software error occurred while initiating subscription request.

Table 182 show subscription local aaa Field Descriptions (continued)

Field	Description
Last error code (continued)	ASNL_SUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED—Subscription expired. ASNL_UNSUBSCRIBE_FAILED —Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR—Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR—Subscriptio n termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR—The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR—Atte mpt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR—Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR—Invalid response was received from the subscription server for the subscription termination request from the client.
notificationMList	String name of the method list of this subscription.
notificationPeriod	• limited—Notifications are started when the first failure status is received while the server is reachable and stopped when the server changes from unreachable to reachable. • infinite—Notifications are started when the subscription begins and stop only when the subscription expires.
notificationType	Type of accounting record for which notification is sent: start, stop, update, or accounting-on.
reportAcctFailure	Indicates whether to send accounting failure responses to the individual application call script before the method list is declared unreachable.
subscription state	When a subscription is completed successfully, the state is notify_acked.

Related Commands

Command	Description
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.

show tbct

To display two b-channel transfer (TBCT) related parameters, use the **show tbct** command in privileged EXEC mode.

show tbct

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1).

Examples

The following is sample output from the **show tbct** command. The fields in the output are self-explanatory.

```
Router# show tbct

TBCT:
        Maximum no. of TBCT calls allowed: No limit
        Maximum TBCT call duration: No limit

There are no TBCT calls currently being monitored.
```

Related Commands

Command	Description
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

show tdm mapping

To display digital signal 0 (DS0) to resource mapping information for a time-division multiplexing (TDM) connection, use the **show tdm mapping** command in user EXEC or privileged EXEC mode.

show tdm mapping [**controller** [**e1** *number*] | **slot** *number*]

Syntax Description

controller	(Optional) Displays information about the T1 or E1 controller.
e1	(Optional) Displays information about the E1 controller.
number	(Optional) Specifies the E1 controller unit number.
slot	(Optional) Displays information about a particular modem card slot.
number	(Optional) Specifies the modem card slot number.

Command Default

If no argument is specified, information for all controllers and slots are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tdm mapping** command. The fields in the display are self-explanatory.

```
Router# show tdm mapping

T1 1/0:1 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------

 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0            DATA
```

```
17        0            DATA
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling

T1 1/0:2 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------

 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0            DATA
17        0            DATA
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling
```

Related Commands

Command	Description
show tdm connections	Displays a snapshot of the TDM bus connection memory in a Cisco access server or displays information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server.

show tgrep neighbors

To display information about the configured Telephony Gateway Registration Protocol (TGREP) neighbors, use the **show tgrep neighbors** command in privileged EXEC mode.

show tgrep neighbors {* | *ip-address*}

Syntax Description

*	Displays all neighbors.
ip-address	IP address of the individual neighbor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tgrep neighbors** command:

```
Router# show tgrep neighbors *

There are 1 nbrs configured

------------------ NBR:192.0.2.0----------------------
TIMERS:
        Keepalive :  Timer Stopped
        Hold Timer :  Timer Stopped
        Connect Retry :  Running, time remaining in ms, 20698


SYNC IN PROGRESS
STATE: TRIPS_IDLE
QUEUES:
        writeQ : 0
        sec_writeQ : 0
        readQ : 0

SOCKET FDs:
prim socket -1, sec socket -1
tgrep_update_version : 0

LAST RESET: USER_INITIATED

Router#
Router#!!!! Trip Connection is setup here...
----------------------- OPEN DUMP BEGINS ------------------------
 0x1 0xFFFFFFFF 0x0 0xFFFFFFB4 0x0
 0x0 0x4 0x58 0x6 0x7
 0xFFFFFF98 0xFFFFFFA9 0x0 0xC 0x0
 0x1 0x0 0x8 0x0 0x2
 0x0 0x4 0x0 0x0 0x0
 0x3
```

```
        Version    :1
        Hold Time    :180
        My ITAD      :1112
        TRIP ID      :101161129

                 Option Paramater #1
                 Param Type: Capability
                 Length 8
                         Cap Code :Send Receive Capability
                         Cap Len  :4
                                  Send Rec Cap: RCV ONLY MODE
        -->All route types supported

----------------------- OPEN DUMP ENDS -----------------------
```

Table 183 describes the significant fields shown in the display.

Table 183 show tgrep neighbors Field Descriptions

Field	Description
TIMERS	Settings for specified timers.
STATE	State of the connection.
QUEUES	The number of writeQ, sec_writeQ, and readQueues are specified in the following three rows.
SOCKET	Socket field description.
LAST RESET	Last reset state.

Related Commands

Command	Description
neighbor (tgrep)	Creates a TGREP session with another device.

show translation-rule

To display the contents of the rules that have been configured for a specific translation name, use the **show translation-rule** command in privileged EXEC mode.

show translation-rule [*name-tag*]

Syntax Description

name-tag	(Optional) Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647.

Command Default

This command gives detailed information about configured rules under a specific rule name. If the name tag is not entered, a complete display of all the configured rules is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.1(1)T	This command was implemented for VoIP on the Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200, and Cisco 7500.
12.1(2)T	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command:

```
Router# show translation-rule

Translation rule address:0x61AB94F8
Tag name:21
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:555.%
```

```
        Sub  pattern:1408555
        Match  type:subscriber
        Sub type:international
**** Xrule rule table *******
        Rule :2
        in_used state:1
        Match pattern:8.%
        Sub  pattern:1408555
        Match  type:abbreviated
        Sub type:international
Translation rule address:0x61C2E6D4
Tag name:345
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:.%555.%
        Sub  pattern:7
        Match  type:ANY
        Sub type:abbreviated
```

Table 184 describes significant fields in this output.

Table 184 show translation-rule Field Descriptions

Translation rule address	Translation rule address in hex.
Tag name	Translation rule tag name.
Translation rule in_used	Translation rule in which the tag is used.
**** Xrule rule table *******	Beginning of the display for a specific rule.
Rule:x	Number of the rule.
in_used state:	Input-searched-pattern.
Match pattern:	Match pattern of the rule.
Sub pattern:	Substituted pattern.
Match type:	Match type.
Sub type:	Substituted pattern match type.

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

show trunk group

To display information for one or more trunk groups, use the **show trunk group** command in user EXEC or privileged EXEC mode.

show trunk group [*name* [**cic**] [**sort** [**ascending** | **descending**]]

Syntax Description

name	(Optional) Trunk group to display.
cic	(Optional) Displays the Circuit Identification Code (CIC) number.
sort	(Optional) Sorts the output by trunk group number, in ascending or descending order.
ascending	(Optional) Specifies ascending display order for the trunk groups. This is the default.
descending	(Optional) Specifies descending display order for the trunk groups.

Command Default

Trunk groups display in ascending order.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(11)T	This command was modified. This command was enhanced to support dial-out trunk groups.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cic** keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Examples

The following sample output shows that for trunk group 1, preemption is enabled, with a preemption tone timer of 10 seconds, and the preemption level is flash.

```
Router# show trunk group 1

Trunk group: 1
        Description:
        trunk group label: 1

        Translation profile (Incoming):
        Translation profile (Outgoing):
```

```
        LPCOR (Incoming): local_group
        LPCOR (Outgoing): local_group

        Preemption is enabled
        Preemption Tone Timer is 10 seconds
        Preemption Guard Timer is 60 milliseconds

        Hunt Scheme is least-used
        Max Calls (Incoming):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Max Calls (Outgoing):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Retries: 0

        Trunk Se0/3/0:15        Preference DEFAULT
                Member Timeslots : 1-5
                Total channels available : 5
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 5
        Trunk Se0/3/1:15        Preference DEFAULT
                Member Timeslots : 1-2
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/0:15        Preference DEFAULT
                Member Timeslots : 1-31
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/1:15        Preference DEFAULT
                Member Timeslots : 1-10
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0

        Total calls for trunk group: Data = 0, Voice = 0, Modem = 0
                                     Pend = 0, Free = 5

        Preemption Call Type:   Active  Pending
                Flash-Override  NA      0
                Flash           0       0
                Immediate       0       0
                Priority        0       0
                Routine         0       0

                Total           0       0

        Active preemption call-type shows the number of calls
        of each priority level which can be preempted by
        higher preemption level calls.

        Pending preemption call-type shows the number of calls
        of each priority level which are pending for the completion
        of call preemption.

        advertise_flag 0x00000040, capacity timer 25 sec tripl_config_mask 0x00000000
        AC_curr 5, FD_curr 0, SD_curr 0

        succ_curr 0 tot_curr 1
        succ_report 0 tot_report 1
        changed 1 replacement position 0
```

Table 185 describes the significant fields shown in the output. Fields are listed in alphabetical order.

Table 185 show trunk group Field Descriptions

Field	Description
Description	Description of the trunk group if entered with the **description** (trunk group) command.
trunk group label	Name of the trunk group.
Translation profile (Incoming)	List of incoming translation profiles.
Translation profile (Outgoing)	List of outgoing translation profiles.
LPCOR (Incoming)	Setting of the **lpcor incoming** command.
LPCOR (Outgoing)	Setting of the **lpcor outgoing** command.
Preemption is	Indicates whether preemption is enabled or disabled.
Preemption level	The preemption level for voice calls to be preempted by a DDR call.
Preemption tone timer	The expiry time for the preemption tone for the outgoing calls being preempted by a DDR call.
Hunt Scheme	Name of the idle channel hunt scheme used for this trunk group.
Max calls (incoming)	Maximum number of incoming calls handled by this trunk group.
Max calls (outgoing)	Maximum number of outgoing calls handled by this trunk group.
Retries	Number of times the gateway tries to complete the call on the same trunk group.
Total calls for trunk group	List of the total calls across all trunks in the trunk group.
Preemption Call Type	List of preemption levels for active and pending calls.
Data	Number of currently used data channels on the trunk or total data calls used by the trunk group.
Free	Number of currently available channels on the trunk or total available calls for the trunk group.
Member timeslots	Member timeslots for this trunk.
Pending	Number of pending channels.
Preference	Preference of the trunk in the trunk group. If DEFAULT appears, the trunk does not have a defined preference.
Total channels available	Number of available channels for the trunk.
Trunk group	ID of the trunk group member.
Voice	Number of currently used voice channels on the trunk or total voice calls used by the trunk group.

Related Commands

Command	Description
description (trunk group)	Includes a specific description of the trunk group interface.
hunt-scheme least-idle	Specifies the method for selecting an available incoming or outgoing channel.
trunk group	Initiates a trunk group definition.
trunk group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

show trunk hdlc

To show the state of the HDLC controllers, use the **show trunk hdlc** command in privileged EXEC mode.

show trunk hdlc {**all** | **ds0** | *slot number*}

Syntax Description

all	Displays information about all the slots with HDLC controllers.
ds0	Displays Ds0 channel availability.
slot	Displays HDLC information about a specific slot.
number	Trunk card slot number.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines The output of the command shows the number of calls on each HDLC controller chip and link. If HDLC calls are failing, this command can help determine if the problem is due to a hardware fault and which controller chip may be responsible.

Examples The following example displays HDLC controller information for all slots:

```
Router# show trunk hdlc all

HDLC Controller information for slot(s): 0 - 13

  Slot 3:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7

  0      0      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a
  0      1      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a

  Slot 12:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7

  0      0      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
  0      1      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
```

Table 186 show trunk hdlc Field Descriptions

Field	Description
Subslot	The DFC slot number upon which the controller resides
HDLC Chip	The chip number within the subslot
HDLC available	The number of HDLC channels available on the chip
ctrlrs total	The total number of HDLC channels on the chip
TDM links	The TDM links connected to the chip
avail DS0s	The number of available DS0s
total DS0s	The total number of DS0s

Related Commands

Command	Description
debug trunk hdlc	Turns on debugging for the HDLC controllers.

show vdev

To display information about the digital signal processors (DSPs) on a specific card, use the **show vdev** command in privileged EXEC mode.

show vdev {*slot*/*port*}

Syntax Description

slot	Slot in which the voice card resides.
port	Port on the voice card.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines This command can be used on the standby and active route switch controller (RSC) to verify that dynamic and bulk synchronization have been performed correctly on a specified port.

Examples The following example shows the output for the last port on a 324 universal port card.

```
Router# show vdev 2/323

flags = 0x0000
dev_status = 0x0000
service = 0x0000
service_type = 0x0
min_speed = 0, max_speed = 0
modulation = 0, err_correction = 0, compression = 0
csm_call_info = 0x0, csm_session = Invalid
vdev_p set to modem_info

DSPLIB information:
dsplib_state = 0x0
dsplib_next_action = 0x0

HDLC information:
call_id = 0x0
called_number =
speed = 0
ces = 0x0
spc = FALSE
d_idb = 0x0

Bulk sync reference = 2, Global bulk syncs = 2
```

Table 186 displays significant fields shown in the output.

Table 186 show vdev Field Descriptions

Field	Description
flags	Internal vdev flags
dev_status	Additional flags giving status of the resource
service	Service currently running on this DSP
service_type	Service type as passed in by RPM
min_speed	Minimum configured modem speed
max_speed	Maximum configured modem speed
modulation	Maximum modulation to be negotiated
err_correction	Error correction to be negotiated
compression	Compression to be negotiated
csm_call_info	Address of the associated csm_call_info structure
csm_session	Session ID as maintained by CSM
vdev_p	Address of the associated resource structure
dsplib_state	State of the resource as seen by the DSPLIB
dsplib_next_action	Next DSPLIB action that should be taken on this resource
call_id	Call identifier if this resource has a HDLC call
called_number	Called number if this resource has a HDLC call
speed	Speed of the connection if this resource has a HDLC call
ces	Circuit emulation service information
spc	True if semi permanent call link
d_idb	Address of the associated D channel idb, if this resource has a HDLC call
Bulk sync reference	Number of times that this resource has been bulk synchronized
Global bulk syncs	Number of bulk synchronizations that the VDEV High Availability client has performed

Related Commands

Command	Description
debug vdev	Turns on debugging for voice devices.
show redundancy	Displays current or historical status and related information on a redundant RSC.

show vfc

To see the entries in the host-name-and-address cache, use the **show vfc** command in privileged EXEC mode.

show vfc *slot-number* [**technology**]

Syntax Description

slot-number	VFC slot number.
technology	(Optional) Displays the technology type of the VFC.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.
12.0(2)XH	The **technology** keyword was added.

Examples

The following is sample output from this command showing that the card in slot 1 is a C549 DSPM:

```
Router# show vfc 1 technology

Technology in VFC slot 1 is C549
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
voice-card	Configures a voice card and enters voice-card configuration mode.

show vfc cap-list

To show the current list of files on the capability list for this voice feature card (VFC), use the **show vfc cap-list** command in user EXEC mode.

show vfc *slot* **cap-list**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Examples

The following is sample output from this command:

```
Router# show vfc 1 cap-list

Capability List for VFC in slot 1:
1. fax-vfc-l.0.1.bin
2. bas-vfc-l.0.1.bin
3. cdc-g729-l.0.1.bin
4. cdc-g711-l.0.1.bin
5. cdc-g726-l.0.1.bin
6. cdc-g728-l.0.1.bin
7. cdc-gsmfr-l.0.1.bin
```

The first line in this output is a general description, stating that this is the capability list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one currently installed in-service file.

Related Commands

Command	Description
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc default-file

To show the default files included in the default file list for a voice feature card (VFC), use the **show vfc default-file** command in user EXEC mode.

show vfc *slot* **default-file**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Examples

The following is sample output from this command:

```
Router# show vfc 1 default-file

Default List for VFC in slot 1:
1. btl-vfc-l.0.13.0.bin
2. cor-vfc-l.0.1.bin
3. bas-vfc-l.0.1.bin
4. cdc-g729-l.0.1.bin
5. fax-vfc-l.0.1.bin
6. jbc-vfc-l.0.13.0.bin
```

The first line in this output is a general description, stating that this is the default list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one default file.

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc directory

To show the list of all files residing on a voice feature card (VFC), use the **show vfc directory** command in user EXEC mode.

show vfc *slot* **directory**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use this command to display a list of all of the files currently stored in Flash memory for a particular VFC.

Examples

The following is sample output from this command:

```
Router# show vfc 1 directory

Files in slot 1  VFC flash:
     File Name                      Size (Bytes)
1 .  vcw-vfc-mz.gsm.VCW             292628
2 .  btl-vfc-l.0.13.0.bin           4174
3 .  cor-vfc-l.0.1.bin              54560
4 .  jbc-vfc-l.0.13.0.bin           16760
5 .  fax-vfc-l.0.1.bin              64290
6 .  bas-vfc-l.0.1.bin              54452
7 .  cdc-g711-l.0.1.bin             190
8 .  cdc-g729-l.0.1.bin             21002
9 .  cdc-g726-l.0.1.bin             190
10.  cdc-g728-l.0.1.bin             22270
11.  cdc-gsmfr-l.0.1.bin            190
```

Table 187 describes significant fields in this output.

Table 187 show vfc directory Field Descriptions

Field	Description
File Name	Name of the file stored in Flash memory.
Size (Bytes)	Size of the file in bytes.

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc version

To show the version of the software residing on a voice feature card (VFC), use the **show vfc version** command in user EXEC mode.

show vfc *slot* **version** {**dspware** | **vcware**}

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.
dspware	Which DSPWare software to display.
vcware	Which VCWare software to display.

Command Modes

Privileged or user EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T with changes to the command output.

Usage Guidelines

Use this command to display the version of the software currently installed in Flash memory on a VFC.

Examples

The following is sample output from this command:

```
Router# show vfc 0 version dspware

Version of Dspware in VFC slot 0 is 0.10
```

The output from this command is a simple declarative sentence stating the version number for the selected type of software (in this example, DSPWare) for the VFC residing in the selected slot number (in this example, slot 0).

Cisco IOS Release 12.2(13)T adds new information to the output of the **show vfc** *slot* **version vcware** and **show vfc** *slot* **version dspware** commands. Messages are output if the Cisco VCWare or DSPWare is not compatible with the Cisco IOS image. The new information is advisory only, so there is no action taken if the software is compatible or incompatible.

If the versions detected fall within the defined criteria and are compatible, nothing is output at bootup time. A confirmation line is output when the **show vfc version vcware** and **show vfc version dspware** commands are used:

```
Router# show vfc 1 version vcware

Voice Feature Card in Slot 1:
VCWare Version     : 7.35
ROM Monitor Version: 1.3
     DSPWare Version    : 3.4.46L
     Technology         : C549
VCWare/DSPWare version compatibility OK
```

Table 188 shows output field descriptions for the **show vfc version vcware** command with compatible firmware.

Table 188 show vfc version vcware Field Descriptions

Field	Description
Voice Feature Card in Slot	Slot in which the VFC is installed.
VCWare Version	Cisco VCWare version. Version 7.35 is the required minimum for Cisco IOS Release 12.2(11)T and higher.
ROM	ROM monitor version shows 1.3.
DSPWare Version	The DSPWare version shows 3.4.46L, which is the required minimum for Cisco IOS Release 12.2(11)T and higher.
Technology	The technology shows C549. C549 technology is available to support either medium-complexity codecs or high-complexity codecs.
VCWare/DSPWare version compatibility	The Cisco VCWare and DSPWare versions are compatible with Cisco IOS software. Cisco VCWare/DSPWare version compatibility is either OK or shows a mismatch. **Note** This option is available only with Cisco IOS Release 12.2(10) mainline and later release or Cisco IOS Release 12.2(11)T and later.

The following is sample outpou from this command.

```
Router# show vfc 1 version dspware

DSPWare version in VFC slot 1 is 3.4.46L
VCWare/DSPWare version compatibility OK
```

Table 189 shows output field descriptions for the **show vfc version dspware** command with compatible firmware.

Table 189 show vfc version dspware Field Descriptions

Field	Description
Voice Feature Card in Slot	Slot in which the VFC is installed.

Table 189 show vfc version dspware Field Descriptions (continued)

Field	Description
DSPWare Version	The DSPWare version shows 3.4.46L, which is the required minimum for Cisco IOS Release 12.2(10)T and higher.
VCWare/DSPWare version compatibility	The Cisco VCWare and DSPWare versions are compatible with Cisco IOS software. Cisco VCWare/DSPWare version compatibility is either OK or shows a mismatch. **Note** This option is available only with Cisco IOS Release 12.2(10) mainline and later or 12.2(11)T and later.

If the found versions are out of range or otherwise mismatched, a representative message is output when you boot up the router or is appended to the output of the **show vfc version vcware** and **show vfc version dspware** commands. Other than the output of these messages, the version check has no other effect, and the software functions normally. The following is an example of when a found version is out of range or mismatched at bootup:

```
...
Firmware version mismatch for bundle AS5300 VCWare
  - version found (6.04) is lower than minimum required (7.35)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.46L)
```

If you were to enter an explicit request, and the software were incompatible, the following output would be displayed:

```
Router# show vfc 1 version vcware

Voice Feature Card in Slot 1:
VCWare Version     : 6.04
ROM Monitor Version: 1.3
     DSPWare Version    : 3.3.10L
     Technology         : C549
Firmware version mismatch for bundle AS5300 VCWare
  - version found (6.04) is lower than minimum required (7.14)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.26L)

Router# show vfc 1 version dspware

DSPWare version in VFC slot 1 is 3.3.10L
Firmware version mismatch for bundle AS5300 VCWare
  - version found (6.04) is lower than minimum required (7.14)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.26L)
```

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.

show video call summary

To display summary information about video calls and the current status of the Video CallManager (ViCM), use the **show video call summary** command in privileged EXEC mode.

show video call summary

Syntax Description

There are no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	The command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to quickly examine the status of current video calls. In Cisco IOS Release 12.0(5)XK and Release 12.0(7)T, there can be only one video call in progress.

Examples

The following example displays information about the ViCM when no call is in progress on the serial interface that connects to the local video codec:

```
Router# show video call summary

Serial0:ViCM = Idle, Codec Ready
```

The following output shows a call starting:

```
Router# show video call summary

Serial0:ViCM = Call Connected
```

The following output shows a call disconnecting:

```
Router# show video call summary

Serial0:ViCM = Idle
```

Related Commands

Command	Description
show call history video record	Displays information about video calls.

show voice accounting method

To display connectivity status information for accounting method lists, use the **show voice accounting method** command in privileged EXEC mode.

show voice accounting method [*method-list-name*]

Syntax Description

method-list-name	(Optional) Name of a specific method list. This option displays connectivity status information for a single method list identified by this argument.

Command Default If no argument is specified, connectivity status information for all accounting method lists is displayed.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Use the **show voice accounting method** command to display the history of status (reachable or unreachable), status transition time, and statistics of the accounting status for a specified accounting method list or all the accounting method lists. A maximum of ten status histories are displayed.

Examples The following is sample output from the **show voice accounting method** command for a specific method list:

```
Router# show voice accounting method ml1

Accounting Method List [ml1]
=======================
Current Status:
---------------
unreachable                [21:52:39 gmt Dec 4 2002]
last record sent time      [23:14:59 gmt Dec 4 2002]
total probe sent out       [84]

Status History:
---------------
(2) unreachable            [21:52:39 gmt Dec 4 2002]
(1) reachable              [21:46:19 gmt Dec 4 2002]
                  SUCCESS                          FAILURE
Record  [Received    | Notified ] [Received    |  Notified  | Reported ]
Type    [from server| to client] [from server|  to client | to call  ]
------  [-----------|----------] [-----------|------------|----------]
START   [     0      |     0    ] [     0      |      0     |     0    ]
UPDATE  [     0      |     0    ] [     0      |      0     |     0    ]
STOP    [     0      |     0    ] [     84     |      84    |     0    ]
ACCT_ON [     0      |     0    ] [     0      |      0     |     0    ]
------  [-----------|----------] [-----------|------------|----------]
```

```
TOTAL   [     0     |     0    ] [     84    |      84    |     0    ]
```

If there is no status history, as in the following example, no status history is displayed.

```
Router# show voice accounting method

Accounting Method List [ml1]
=====================
Current Status:
---------------
reachable                   [21:52:39 gmt Dec 4 2002]
last record sent time       [23:14:59 gmt Dec 4 2002]
total probe sent out        [2]

                SUCCESS                          FAILURE
Record  [Received    | Notified ] [Received    |  Notified  | Reported ]
Type    [from server| to client] [from server|  to client  | to call  ]
------  [-----------|----------] [-----------|------------|----------]
START   [     0     |     0    ] [     0     |       0    |     0    ]
UPDATE  [     0     |     0    ] [     0     |       0    |     0    ]
STOP    [     0     |     0    ] [     2     |       2    |     0    ]
ACCT_ON [     0     |     0    ] [     0     |       0    |     0    ]
------  [-----------|----------] [-----------|------------|----------]
TOTAL   [     0     |     0    ] [     2     |       2    |     0    ]
```

Table 190 describes the significant fields shown in the display.

Table 190 show voice accounting method Field Descriptions

Field	Description
Current Status: reachable or unreachable	Current status of the method list: reachable or unreachable and the time (in hh:mm:ss) and date the method list reached this status.
last record sent time	Time (in hh:mm:ss) and date the last accounting record was sent to the method list.
total probe sent out	Number of probe records sent up to the time of the show command.
SUCCESS: Received from server	Number of success status of the accounting records of this type received from the method list.
SUCCESS: Notified to client	Number of success status of the accounting records of this type for which notifications were sent to the GAS.
FAILURE: Received from server	Number of failure status of the accounting records of this type received from the method list.
FAILURE: Notified to client	Number of failure status of the accounting records of this type for which notifications were sent to the GAS.
FAILURE: Reported to call	Number of failure status of the accounting records of this type that were reported to the call application.

Related Commands

Command	Description
clear voice accounting method	Clears accounting status statistics for a particular accounting method list or all accounting method lists.

show voice accounting response pending

To display information regarding pending VoIP AAA accounting responses, use the **show voice accounting response pending** command in privileged EXEC mode.

show voice accounting response pending

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example displays information regarding pending VoIP AAA accounting responses:

```
Router# show voice accounting response pending

Total num of acct sessions waiting for acct responses: 0
Total num of acct start responses pending:             0
Total num of acct interim update responses pending:     0
Total num of acct stop responses pending:              0
```

Table 191 lists and describes the significant output fields.

Table 191 show voice accounting response pending Field Descriptions

Field	Description
Total num of acct sessions waiting for acct responses	Number of accounting sessions that are waiting for accounting responses.
Total num of acct start responses pending	Number of accounting start responses that are pending.
Total num of acct interim update responses pending	Number of accounting interim update responses that are pending.
Total num of acct stop responses pending	Number of accounting stop responses that are pending.

show voice busyout

To display information about the voice-busyout state, use the **show voice busyout** command in privileged EXEC mode.

show voice busyout

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command displays the following information:

- Interfaces that are being monitored for busyout events
- Voice ports currently in the busyout state and the reasons

Examples

The following is sample output from this command:

```
Router# show voice busyout

If following network interfaces are down, voice port will be put into busyout state
ATM0
Serial0
The following voice ports are in busyout state

1/1     is forced into busyout state
1/2     is in busyout state caused by network interfaces
1/3     is in busyout state caused by ATM0
1/4     is in busyout state caused by network interfaces
1/5     is in busyout state caused by Serial0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port in the busyout monitor state.
busyout seize	Changes the busyout seize procedure from a voice port.
voice-port busyout	Places all voice ports associated with a serial or ATM interface in a busyout state.

show voice call

To display the call status for voice ports on the Cisco router, use the **show voice call** command in user EXEC or privileged EXEC mode.

Cisco 827, Cisco 1700 Series, and Cisco 7750 with Analog Voice Ports

show voice call [*slot*/*port* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco 2600, Cisco 3600, Cisco 3700 Series with Analog Voice Ports

show voice call [*slot*/*subunit*/*port* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco 2600, Cisco 3600, and Cisco 3700 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

show voice call [*slot*/*port*:*ds0-group* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco 7200 Series, and Cisco 7500 Series with Digital Voice Ports

show voice call [*slot*/*port*:*ds0-group* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

:

Syntax Description

Cisco 827, Cisco 1700 Series, and Cisco 7750 with Analog Voice Ports	
slot/*port*	(Optional) A specific analog voice port: • *slot*—Physical slot in which the analog voice module (AVM) is installed. • /*port*—Analog voice port number. Range is from 1 to 6. The slash mark is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command displays the status of a specific call.
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port, regardless of port activity.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series with Analog Voice Ports	
slot/*subunit*/*port*	(Optional) A specific analog voice port: • *slot*—Router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • /*subunit*—Voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) The slash mark is required. • /*port*—Analog voice port number. Valid entries are 0 and 1. The slash mark is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command displays the status of a specific call.

sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port, regardless of port activity.

Cisco 2600, Cisco 3600, and Cisco 3700 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)	
slot/*port*:*ds0-group*	(Optional) A specific digital voice port: • *slot*—Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • /*port*—T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • :*ds0-group*—T1 or E1 logical port number. Range is from 0 to 23 for T1 and from 0 to 30 for E1. The colon is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command shows the status of a specific call.
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the DSP port regardless of port activity.

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco 7200 Series, and Cisco 7500 Series with Digital Voice Ports	
slot/*port*:*ds0-group*	(Optional) A specific digital voice port: • *slot*—Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • /*port*—T1 or E1 physical port in the VWIC. Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • :*ds0-group*—T1 or E1 logical port number. Range is from 0 to 23 for T1 and from 0 to 30 for E1. The colon is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command shows the status of a specific call.
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port regardless of port activity.

Command Modes

User EXEC
privileged EXEC

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(13)T	This command was modified with the **status**, *call-id*, and **sample** *seconds* command options. This command is available on all voice platforms.
12.4(3d)	This command was modified to support the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms for Non-Facility Associated Signaling (NFAS) configuration. Output was modified to provide accurate port information for NFAS configuration on these platforms.
15.1(3)T	This command was modified. The output of this command was enhanced to display the connection status of foreign exchange office (FXO) ports.

Usage Guidelines

This command works on Voice over Frame Relay, Voice over ATM, and Voice over IP by providing the status at the following levels of the call-handling module:

- Call-processing state machine
- End-to-end call manager
- Protocol state machine
- Tandem switch

Note This command is not supported in Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms for NFAS configuration before Cisco IOS Release 12.4(3d).

This command displays call-processing and protocol state-machine information for a voice port if the information is available. This command also shows information on the DSP channel associated with the voice port if the information is available. All real-time information in the DSP channel, such as jitter and buffer overrun, is queried to the DSP channel, and asynchronous responses are returned to the host side.

If no call is active on a voice port, the **show voice call summary** command displays only the VPM (shutdown) state. If a call is active on a voice port, the **show voice call summary** command displays voice telephony service provider (VTSP) state. For an on-net call or a local call without local bypass (not cross-connected), the codec and voice activity detection (VAD) fields are displayed. For an off-net call or a local call with local bypass, the codec and VAD fields are not displayed.

When a call is active on a voice port, the **show voice call summary** command displays the VTSP state. The VTSP state always shows the VTSP signaling state irrespective of the type of call: voice call or a fax call. A fax call does not display S_Fax. The following output is displayed:

```
PORT            CODEC    VAD VTSP STATE             VPM STATE
=============== ======== === ==================== ======================
1/0:1.1          1          y  S_CONNECT              EM_CONNECT
```

Note Use the **show voice dsmp stream** command to display the current session of the voice Distributed Stream Media Processor (DSMP) media stream and its related applications.

The **show voice call** command does not display the codec and VAD fields because this information is in the summary display. If you use the **show voice call status** command by itself, an immediate list of all the active calls is shown. You can use the *call-id* argument to request that the DSP associated with the *call-id* be queried for run-time statistics twice, once immediately, and a second time after **sample** *seconds*.

The **sample** *seconds* is the number of seconds over which the status is to be determined. The results of the run-time statistic queries are then analyzed and presented in a one-line summary format.

When a call terminates during the specified sample period, the following output message is returned:

```
CallID call id cannot be queried
CallID call id second sample responses unavailable
```

Note The Voice Call Tuning feature is not supported on the Cisco AS5300.

Examples

The following is sample output from the **show voice call summary** command showing two local calls connected without local bypass:

```
Router# show voice call summary

PORT    CODEC    VAD VTSP STATE             VPM STATE
======= ======== === ===================== ========================
0:17.18                                     *shutdown*
0:18.19 g729ar8   n  S_CONNECT             FXOLS_OFFHOOK
0:19.20                                     FXOLS_ONHOOK
0:20.21                                     FXOLS_ONHOOK
0:21.22                                     FXOLS_ONHOOK
0:22.23                                     FXOLS_ONHOOK
0:23.24                                     EM_ONHOOK
1/1                                         FXSLS_ONHOOK
1/2                                         FXSLS_ONHOOK
1/3                                         EM_ONHOOK
1/4                                         EM_ONHOOK
1/5                                         FXOLS_ONHOOK
1/6     g729ar8   n  S_CONNECT             FXOLS_CONNECT
```

The following is sample output from the **show voice call summary** command showing two local calls connected with local bypass:

```
Router# show voice call summary

PORT    CODEC    VAD VTSP STATE             VPM STATE
======= ======== === ===================== ========================
0:17.18                                     *shutdown*
0:18.19              S_CONNECT              FXOLS_OFFHOOK
0:19.20                                     FXOLS_ONHOOK
0:20.21                                     FXOLS_ONHOOK
0:21.22                                     FXOLS_ONHOOK
0:22.23                                     FXOLS_ONHOOK
0:23.24                                     EM_ONHOOK
1/1                                         FXSLS_ONHOOK
1/2                                         FXSLS_ONHOOK
1/3                                         EM_ONHOOK
1/4                                         EM_ONHOOK
1/5                                         FXOLS_ONHOOK
1/6                  S_CONNECT              FXOLS_CONNECT
```

The following is sample output from the **show voice call summary** command in which the connected FXO port 0/2/0 shows status of "FXOLS_ONHOOK" whereas the FXO port 0/2/1, which is disconnected, shows a status of "FXOLS_BUSYOUT":

```
Router# show voice call summary

PORT            CODEC     VAD VTSP STATE             VPM STATE
=============== ========= === ==================== ======================
0/0/0          -          -  -                      FXSLS_ONHOOK
0/0/1          -          -  -                      FXSLS_ONHOOK
0/3/0:23.1       -          -  -
0/3/0:23.2       -          -  -
.
.
.
0/3/0:23.23      -          -  -
0/1/0          -          -  -                      DID_ONHOOK
0/1/1          -          -  -                      DID_ONHOOK
0/2/0          -          -  -                      FXOLS_ONHOOK
0/2/1          -          -  -                      FXOLS_BUSYOUT
2/0/0          -          -  -                      FXSLS_ONHOOK
2/0/1          -          -  -                      FXSLS_ONHOOK
2/0/2          -          -  -                      FXSLS_ONHOOK
2/0/3          -          -  -                      FXSLS_ONHOOK
2/0/4          -          -  -                      FXSLS_ONHOOK
2/0/5          -          -  -                      FXSLS_ONHOOK
2/0/6          -          -  -                      FXSLS_ONHOOK
2/0/7          -          -  -                      FXSLS_ONHOOK
```

Note Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports—any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to "up" for FXO port 0/2/0:

```
000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0,
changed state to operational status up due to cable reconnection
```

The following is sample output from the **show voice call summary** command showing one regular PRI port and one NFAS PRI port on a Cisco AS5350, Cisco AS5400, or Cisco AS5850 platform. Port 3/2:D belongs to a regular PRI voice port with time slots 0 and 22. Port Se3/1 belongs to an NFAS PRI voice port with time slots 0,1, and 2 on T1 controller 3/1, which is a member of an NFAS group.

In the case of NFAS on Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms, the port is reported in terms of the serial interface associated with the T1 controller, and the time slot is counted from 0 (for example, 0, 1, 2, 3).

```
Router# show voice call summary

PORT            CODEC    VAD VTSP STATE             VPM STATE
=============== ======== === ==================== ======================
3/2:D.0         None      y  S_ALERTING            S_TSP_INCALL
3/2:D.22        None      y  S_ALERTING            S_TSP_INCALL
Se3/1:0         None      y  S_CONNECT             S_TSP_CONNECT
Se3/1:1         None      y  S_CONNECT             S_TSP_CONNECT
Se3/1:2         None      y  S_CONNECT             S_TSP_CONNECT
```

Note The output from the **show voice call summary** command is slightly different in the PORT field on platforms other than the Cisco AS5350, Cisco AS5400, and Cisco AS5850. The contrast between platform types is as follows:

Platform	Regular PRI (T1)	NFAS PRI (T1)*
non-AS5xxx	3/0:23.TS	3/1:23.TS
AS5xxx	3/0:D.TS	Ser3/1:(TS-1)

* Assumes T1 3/1 is a member of an NFAS group with T1 3/0 as the primary NFAS member, and TS is the time slot counted from a base of 1 (for example 1, 2, 3).

The following is sample output from the **show voice call** command for analog voice ports:

```
Router# show voice call

1/1 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/2 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/3 is shutdown
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
1/5 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
1/6 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP

Router# show voice call 1/4

1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
router#    ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 1445779863, Rx Delay Est(ms): 95
Rx Delay Lo Water Mark(ms): 95, Rx Delay Hi Water Mark(ms): 125
       ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 10, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
Buf Overflow Discard(ms): 20, Talkspurt Endpoint Detect Err: 0
       ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 537, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 50304730, Rx Vox Dur(ms): 16090, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
       ***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 567, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 50304730, Tx Vox Dur(ms): 17010, Tx Fax Dur(ms): 0
       ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
       ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -70.3 from PBX/Phone, Tx -68.0 to PBX/Phone
TDM ACOM Levels(dBm0): +2.0, TDM ERL Level(dBm0): +5.6
TDM Bgd Levels(dBm0): -71.4, with activity being voice
```

The following is sample output from the **show voice call** command for analog voice ports on a Cisco 7200 series. The output includes the DSPfarm, T1 interface, and DS0 or TLM slot configuration:

```
Router# show voice call 6/0:0

6/0:0 1 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 2 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 3 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 4 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 5 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 6 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 7 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 8 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 9 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 10-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 11-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 12-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
```

The following is sample output from the **show voice call status** command on the Cisco 2600 series. You can use this command rather than the **show call active brief** command to obtain the caller ID; the caller ID output of the **show voice call status** command is already in hexadecimal form.

```
Router# show voice call status

CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x1        11CE 0x02407B20 1:0.1     1/1     1000       g711ulaw 2000/1000
1 active call found
```

Using the *call-id* argument is a generic means to identify active calls. If the *call-id* is omitted, the query shows all active voice calls. In the following example, a list of all active calls with relevant identifying information is shown:

```
Router# show voice call status

CallID    CID    ccVdb       Port     DSP/Ch  Called #   Codec    Dial-peers
0x3       11D4   0x62972834  1/0/0    1/1      10001     g711ulaw 1/2
0x4       11D4   0x62973AD0  1/0/1    2/1     *10001     g711ulaw 2/1
0xA       11DB   0x62FE9D68  1/1/0    3/1     *2692      g729r8   0/2692
2 active calls found
```

Note You can query only one call at a time. If you attempt queries from different ports (console and Telnet), and if a query is in progress on another port, the system asks you to wait for completion of that query. You can query any call from anywhere, at anytime, except during the sample interval for an enquiry that is already in progress. This simplifies the implementation significantly and does not reduce the usefulness of the command.

The following example shows echo-return-loss (ERL) reflector information where the call ID is 3 and the sample period is 10 seconds:

```
Router# show voice call status 3 sample 10

Gathering information (10 seconds)...
CallID    Port     DSP/Ch  Codec    Rx/Tx     ERL         Jitter
0x3       1/0/0    1/1     g711ulaw 742/154   5.6         50/15
```

In this example, ERL is the echo return loss (in dB) as reported by the DSP. Jitter values are the current delay and the jitter of the packets around that delay.

If the router is running the extended echo canceller, output looks similar to the following if you enter the same command. The output shows a new value under ERL/Reflctr: the time difference, in ms, between the original signal and the loudest echo (peak reflector) as detected by the echo canceller:

```
Router# show voice call status 3 sample 10

Gathering information (10 seconds)...
CallID    Port     DSP/Ch  Codec    Rx/Tx     ERL/Reflctr Jitter
0x3       1/0/0    1/1     g711ulaw 742/154   5.6/12      50/15
```

The following examples show output using the NextPort version of the standard echo canceller. (Time-slot information is also in the output for digital ports.)

```
Router# show voice call status

CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x97       12BB 0x641B0F68 3/0:D.1   1012/2  31001      g711ulaw 3/31000
0x99       12BE 0x641B0F68 3/0:D.2   1012/3  31002      g711ulaw 3/31000
2 active calls found

Router# show voice call status

CallID     CID  ccVdb       Port     DSP/Ch  Called #   Codec    Dial-peers
0x2        11D1 0x62FE6478 1/0/0     1/1     10001      g711ulaw 1/2
0x3        11D1 0x62FE80F0 1/0/1     2/1    *10001      g711ulaw 2/1
1 active call found
```

When using the **test call id** command, you must specify a call ID, which you can obtain by using the **show voice call status** command. The following is an example of how to obtain the call ID for use as the *call-id* argument. The first parameter displayed in the output is the call ID.

Note Do not use the 0x prefix in the *call-id* argument when you enter the resulting call ID in the **test call status** command.

The following shows keyword choices when using the **show voice call** command with the | (pipe) option:

```
Router# show voice call | ?

  append    Append redirected output to URL (URLs supporting append operation
            only)
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output to a URL
  tee       Copy output to a URL
```

Table 192 describes significant fields shown in the previous displays.

Table 192 show voice call Field Descriptions

Field (listed alphabetically)	Description
Called #	Called number. • No "*" before the number denotes an originating call leg. Two of the call legs in the example constitute one locally switched call and one network call, so the call legs refer to two active calls. • A "*" before the number denotes a destination call leg (for example, this number was called with Called #).
CallID	This hexadecimal number used for further query is the monotonically increasing number that call control maintains for each call leg (ccCallID_t).
ccVdb	Value that is displayed in many other debugs to identify these call legs.
CID	Conglomerate value derived from the GUID that appears in the **show call active brief** command.
Codec	Codec.
Dial-peers	Dial peer.
DSP/Ch	DSP and channel allocated to this call leg. The format of these values is platform dependent (particularly the Cisco AS5300, which shows the DSP number as a 3-digit number, <VFC#><DSPM#><DSP#>). Time-slot information is also in the output for digital ports. For example, if you are using a digital port, the time slot is also returned: dsp/ch/time slot.
ERL	Echo return loss (in dB).
ERL/Reflctr	Time difference, in ms, between the original signal and the loudest echo (peak reflector) as detected by the echo canceller.
Jitter	Current values of the delay and the jitter of the packets around that delay.
Port	Voice port.
Rx/Tx	Transmit and receive rates for the connection.
VAD	Voice-activity detection: y or n.
VPM STATE	Voice-port-module (VPM) state.
VTSP STATE	Voice-telephony-service-provider (VTSP) state.

For more information about the extended echo canceller, see *Extended ITU-T G.168 Echo Cancellation*.

Related Commands

Command	Description
show call active brief	Displays a summary of active call information.

show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsmp stream	Displays the current session of the voice DSPM media stream.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
test call id	Manipulates the echo canceller and jitter buffer parameters in real time.

show voice cause-code

To display error category to Q.850 cause code mapping, use the **show voice cause-code** command in user EXEC mode.

show voice cause-code category-q850

Syntax Description

category q850	Displays error category to Q.850 cause code mapping.

Command Default No default behavior or values.

Command Modes User EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines Use this command to display the internal error category to Q.850 cause code mapping table, and configured and default values, with category descriptions.

Examples The following example displays Q.850 cause code mapping:

```
Router# show voice cause-code category-q850

The Internal Error Category to Q850 cause code mapping table:-

 Error Configured Default    Description
Category  Q850     Q850
   128     27        3  Destination address resolution failure
   129     38      102  Call setup timeout
   178     41       41  Internal Communication Error
   179     41       41  External communication Error
   180     47       47  Software Error
   181     47       47  Software Resources Unavailable
   182     47       47  Hardware Resources Unavailable
   183     41       41  Capability Exchange Failure
   184     49       49  QoS Error
   185     41       41  RTP/RTCP receive timer expired or bearer layer failure
   186     38       38  Signaling socket failure
   187     38       38  Gateway or signaling interface taken out of service
   228     50       50  User is denied access to this service
   278     65       65  Media Negotiation Failure due to non-existing Codec
```

Table 193 describes the significant fields shown in the display.

Table 193 show voice cause-code Field Descriptions

Field	Description
128	Destination address resolution failure
129	Call setup timeout
178	Internal communication error
179	External communication Error
180	Software error
181	Software resources unavailable
182	Hardware resources unavailable
183	Capability exchange failure
184	QoS error
185	RTP/RTCP receive timer expired or bearer layer failure
186	Signaling socket failure
187	Gateway or signaling interface taken out of service
228	User denied access to this service
278	Media negotiation failure due to non existing codec

Related Commands

Command	Description
error-category q850-cause	Specifies Q.850 cause code mapping

show voice class called-number

To display a specific voice class called-number, use the **show voice class called-number** command in privileged EXEC mode.

show voice class called-number [**inbound** | **outbound**] *tag*

Syntax Description

inbound	Displays the specified inbound voice class called-number.
outbound	Displays the specified outbound voice class called-number.
tag	Digits that identify this voice class called-number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display a specific inbound or outbound voice class called-number.

Examples

The following is sample output from this command:

```
Router# show voice class called-number outbound 200
Called Number Outbound: 200
           index 1      4085550100
           index 2      4085550102
           index 3      4085550103
           index 4      4085550104
```

Table 194 describes significant fields shown in the display.

Table 194 show voice class called-number Field Descriptions

Field	Description
Called Number Inbound/Outbound	The tag for the specified inbound or outbound voice class called-number.
index *number*	The number or range of numbers for this voice class called number.

Related Commands

Command	Description
show voice class called-number-pool	Displays voice class called number pool configuration information.

show voice class called-number-pool

To display a voice class called-number pool, use the **show voice class called-number-pool** command in privileged EXEC mode.

show voice class called-number-pool tag [**detail**]

Syntax Description

tag	Digits that identify this voice class called-number-pool. Range is 1 to 10000.
detail	Displays idle called number and allocated called number information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display the voice class called number pool configuration information. The **detail** keyword displays up to 16 idle called numbers, and up to 4 allocated called numbers for each allocated request.

Examples

The following sample output displays configuration information for voice class called-number-pool 100, including idle called numbers and allocated called numbers:

```
Router(config)# show voice class called-number-pool 100 detail

Called Number Pool: 100
index 1 100A11 - 100A20
index 2 200#55 - 200#77
index 3 5551111 - 6662333
index 99 123C11 - 123C99
All called numbers are generated from table: FALSE
No of idle called numbers: 16
List of idle called numbers:
100A11 100A12 .. Display up to 16 idle called number from the pool
100A13 100A14
100A15 100A16
100A17 100A18
100A19 100A20
200#55 200#56
200#57 200#58
200#59 200#60
No of alloc requests : 1
Ref Id Alloc PC Size
2 41F84190 16
List of alloc called numbers: .. Display the first 4 allocated called number for RefId 2
200#61 200#62
200#63 200#64
```

Table 195 describes significant fields shown in the display.

Table 195 show voice class called-number-pool Field Descriptions

Field	Description
Called Number Pool	Tag that identifies the called number pool.
index	Number or range of numbers for this called number pool.
All called numbers are generated from table	• FALSE—Numbers are not generated from called number table. • TRUE—Numbers are generated from called number table.
No. of idle called numbers	Number of idle called numbers in the called number pool.
List of idle called numbers	List of idle numbers in the called number pool.
No. of alloc requests	Number of requests for numbers from the called number pool.
Ref Id Alloc PC Size	Reference ID for a specific list of allocated numbers.
List of alloc called numbers	List of first four allocated numbers from the called number pool.

Related Commands

Command	Description
show voice class called-number	Displays a specific voice class called-number.

show voice class resource-group

To display the resource group configuration information for a specific resource group or all resource groups, use the **show voice class resource-group** command in privileged EXEC mode.

show voice class resource-group {*tag* | **all**}

Syntax Description

tag	Unique tag for the resource group.
all	Displays information for all voice resource groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

You can use the **show voice class resource-group** command to display the parameters configured to monitor resources.

Examples

The following is sample output from the **show voice class resource-group** command:

```
Router> enable
Router# show voice class resource-group 2

Resource Availability Indicator status
Resource Index 2

Resource Type:SYSTEM
         Status: Low threshold
Resource Type: MEM Subtype: io-mem Low/High watermark: 2/5
         Status: Low threshold
Report Interval 34
------------------------------------------------------------
```

Table 196 describes the significant fields shown in the display.

Table 196 show voice class resource-group Field Descriptions

Field	Description
Resource Index	Unique index value to identify the resource group.
Resource Type	Type of the resource being monitored.
Status	Status of the resource.

Table 196 show voice class resource-group Field Descriptions (continued)

Field	Description
Subtype	Subtype of the resource being monitored.
Report Interval	Periodic reporting interval for the resource being monitored. The status of the resource being monitored is reported based on the preconfigured timer value.

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

show voice class uri

To display summary or detailed information about configured uniform resource identifier (URI) voice classes, use the **show voice class uri** command in user EXEC or privileged EXEC mode.

show voice class uri [*tag* | **summary**]

Syntax Description

tag	(Optional) Specific URI voice class for which to display detailed information.
summary	(Optional) Displays a short summary of all URI voice classes.

Command Default

Detailed information about the configured URI voice classes is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The command was enhanced to display the mutiple hosts in the configured URI classes.

Usage Guidelines

If both the *tag* argument and **summary** keyword are omitted, the output displays detailed information about all URI voice classes.

Examples

The following is sample output from this command:

```
Router# show voice class uri

Voice URI class: 100
    SNMP status = Active
    Schema = sip
    pattern = 12345

Voice URI class: 101
    SNMP status = Active
    Schema = sip
    pattern = 555....

Voice URI class: 102
    SNMP status = Active
    Schema = sip
    user-id = demo
    host = cisco
    phone context =

Voice URI class: 103
```

```
    SNMP status = Active
    Schema = tel
    phone number = 555....
    phone context =

Voice URI class: 700
     SNMP status = Active
     Schema = sip
     pattern = elmo@sip.tgw.com*

Voice URI class: 104
     SNMP status = Active
     Schema = tel
     pattern = 5550134

Voice URI class: 700
     SNMP status = Active
     Schema = sip
     user-id =
     host = exmp.example.com
     phone context =

     host instances:
      ipv4:192.168.0.1
      ipv6:[2001:0DB8:0:1:FFFF:1234::5]
      dns:ogw.example.com
```

The following is sample output from this command with the **summary** keyword:

```
Router# show voice class uri summary

_____________________________________________________________
Class Name                      Schema         SNMP
-------------------------------------------------------------
100                             sip            Active
101                             sip            Active
102                             sip            Active
103                             tel            Active
700                             sip            Active
104                             tel            Active
_____________________________________________________________
```

Table 197 describes the significant fields in the displays.

Table 197 show voice class uri Field Descriptions

Field	Description
Class Name	Tag that identifies the URI voice class.
Schema	Whether the voice class is used for SIP or TEL URIs.
pattern	Pattern used to match the entire SIP or TEL URI as configured with the **pattern** command.
user-id	Pattern used to match the user-id field in the SIP URI as configured with the **user-id** command.
host	Pattern used to match the host field in the SIP URI with the **host** command.
phone number	Pattern used to match the phone number field in a TEL URI as configured with the **phone number** command.
phone context	Pattern used to match the phone context field in a SIP or TEL URI as configured with the **phone context** command.

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

show voice connectivity summary

To display the results of the last connectivity checks performed on all analog Foreign Exchange Station (FXS) ports on a router, use the **show voice connectivity summary** command in privileged EXEC mode.

show voice connectivity summary

Syntax Description This command has no arguments or keywords.

Command Default A summary of the last connectivity checks performed on all analog FXS ports on a router is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Examples The following example shows how the **show voice connectivity summary** command is used:

```
Router> enable
Router# show voice connectivity summary
.
.
.
! The summary results include information such as the port address, type of connectivity
! check performed, result of connectivity check for each port
```

show voice data

To display the call control application programming interface (CCAPI) and Telephony Service Provider (VTSP) data structures, use the **show voice data** command in user EXEC or privileged EXEC mode.

show voice data {**ccapi** {**ccCallEntry** {*call-id* | **all**} | **ccCallInfo**} | **vtsp** {**ccCallInfo** | **vtsp_cdb** {*call-id* | **all**} | **vtsp_sdb** {*call-id* | **all**}}

Syntax Description

ccapi	Displays all the CCAPI calls.
ccCallEntry	Displays the call entry.
call-id	Call identifier (ID) in the range 1 to 4294967295.
all	Displays all the call entries.
ccCallInfo	Displays the call information.
vtsp	Displays all the VTSP calls.
vtsp_cdb	Displays all the VTSP call control back calls.
vtsp_sdb	Displays all the VTSP signalling data block calls.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **show voice data** command:

```
Router# show voice data ccapi ccCallEntry all

CallEntry=0x6B8051B0; CallID=7(0x7)::

element:{ 0x6B8051B0; 0x6B8051B4; 0x6B8051B8; } 7; <appReturnStack>; 1735408; 1;
0x6B8051D8; 7; 8; callInfo:{ 0; 112233; <NULL>; 889988; <NULL>; <NULL>; <NULL>;
<NULL>; <NULL>; <NULL>; FALSE; FALSE; TRUE; <NULL>; 0; 0; 0; <NULL>; RegularLine; Unknown;
D356CC33-E54B-11D7-8005-00169D6EE1AE; D356CC33-E54B-11D7-8005-00169D6EE1AE; 0; 0; 0; 0; 0;
998877; 0x6B80547C; 0; TRUE; FALSE; 0.0.0.0; 0.0.0.0; 0x6B8054A0; 0x6B8054A4; 0x6B8054A8;
0x6B8054AC; 0; FALSE; FALSE; 0x6B8054BC; 0; call_decode:{ redirect_info:{ 0xFF; 0xFF;
0xFF; 0xFF; 0xFF; 0xFF; 0x00; 0xFF; 255; <NULL>; <NULL>; 0x00; FALSE; FALSE; } 0x00; 0x80;
0x00; 0x80; 0; 0x00; <NULL>; 0; 0x00; <NULL>; FALSE; FALSE; FALSE; FALSE; -1; <NULL>;
TRUE; <transfer_info>; FALSE; 129; 40; 104; 0xFF; TRUE; } FALSE;
D357685B-E54B-11D7-8016-CB962D72A90A; 0; 0; 0; 0; 0; 0; 0x6B805634; FALSE; <NULL>; FALSE;
FALSE; FALSE; 0; 0; 0; <NULL>; ISDN 7/0:1:D; FALSE; FALSE; FALSE; 0x00; <NULL>; <NULL>;
0x6B80585C; 0; 0x6B805864; } 0x6B805914; 0x6B805918; 0x6B80591C; 0x6B805920;
<altAssocList>; FALSE; 0x6B80593C; 0x6B805940; 0x6B805944; FALSE; 0; 65535; TRUE; 0;
FALSE; 1; <disconnect_timer>; <inter_digit_timer>; 10000; <initial_timer_timestamp>;
10000; FALSE; 0; 0; -1; <NULL>; 0x6B8059F8; <evCategoryMask>; <evDetailMask>; 4294967295;
0x6B805C48; FALSE; 0; 0; TRUE; TRUE; TRUE; 0; 0; 0x6B805C6C; FALSE; 0; 4; 0; -1; FALSE;

CallEntry=0x6B805C90; CallID=8(0x8)::
```

```
element:{ 0x6B805C90; 0x6B805C94; 0x6B805C98; } 8; <appReturnStack>; 1735408; 2;
0x6B805CB8; 8; 7; callInfo:{ 0; 112233; <NULL>; 889988; <NULL>; 112233; 112233; <NULL>;
<NULL>; <NULL>; <NULL>; FALSE; FALSE; TRUE; <NULL>; 0; 0; 0; <NULL>; RegularLine; Unknown;
D356CC33-E54B-11D7-8005-00169D6EE1AE; D356CC33-E54B-11D7-8005-00169D6EE1AE; 7; 0; 0; 0; 2;
112233; 0x6B805F5C; 0; FALSE; FALSE; 0.0.0.0; 0.0.0.0; 0x6B805F80; 0x6B805F84; 0x6B805F88;
0x6B805F8C; 0; FALSE; FALSE; 0x6B805F9C; 0; call_decode:{ redirect_info:{ 0xFF; 0xFF;
0xFF; 0xFF; 0xFF; 0xFF; 0x00; 0xFF; 255; <NULL>; <NULL>; 0x00; FALSE; FALSE; } 0x00; 0x80;
0x00; 0x00; 0; 0x00; <NULL>; 0; 0x00; <NULL>; FALSE; FALSE; FALSE; FALSE; -1; <NULL>;
TRUE; <transfer_info>; FALSE; 129; 40; 104; 0xFF; TRUE; } FALSE;
D357685B-E54B-11D7-8016-CB962D72A90A; 0; 0; -1; 0; 0; 0; 0x6B806114; FALSE; <NULL>; FALSE;
FALSE; FALSE; 0; 0; 0; <NULL>; ISDN 7/0:1:D; TRUE; FALSE; FALSE; 0x00; <NULL>; <NULL>;
0x6B80633C; 0; 0x6B806344; } 0x6B8063F4; 0x6B8063F8; 0x6B8063FC; 0x6B806400;
<altAssocList>; FALSE; 0x6B80641C; 0x6B806420; 0x6B806424; FALSE; 0; 65535; FALSE; 0;
FALSE; 1; <disconnect_timer>; <inter_digit_timer>; 10000; <initial_timer_timestamp>;
10000; FALSE; 0; 0; -1; <NULL>; 0x6B8064D8; <evCategoryMask>; <evDetailMask>; 4294967295;
0x6B806728; FALSE; 0; 0; TRUE; TRUE; TRUE; 0; 0; 0x6B80674C; FALSE; 0; 4; 0; -1; FALSE;
```

Table 198 describes the significant fields shown in the display.

Table 198 show voice data Field Descriptions

Field	Description
CallEntry	Displays the call entry identification number used for the incoming call leg.
CallID	Displays the specified call identifier value.
element	Indicates the various configuration values for the service element.
callInfo	Displays the call informaton.
call_decode	Displays the status of the audio decoder.
redirect_info	Displays the forwarding request information when a call is being forwarded.
transfer_info	Displays the call transfer request information.
disconnect_timer	Displays the timeout value, in seconds, specified to disconnect the call.
inter_digit_timer	Displays the maximum allowable time, in seconds, between digits dialed by the user.

Related Commands

Command	Description
debug voip ccapi error	Traces error logs in the call control API.

show voice dnis-map

To display current dialed-number identification service (DNIS) map information, use the **show voice dnis-map** command in privileged EXEC mode.

show voice dnis-map [*dnis-map-name* | **summary**]

Syntax Description

dnis-map-name	(Optional) Name of a specific DNIS map.
summary	(Optional) Displays a short summary of each DNIS map.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command displays a detailed description of each configured DNIS map.

If the name of a specific DNIS map is entered, the command displays detailed information about only that DNIS map.

If the **summary** keyword is used, the command displays a one-line summary about each DNIS map.

If an asterisk is displayed next to a DNIS map name when the **summary** keyword is used, it means that the DNIS map is configured, but not running. Normally this is because the external text file was not successfully loaded, for example:

```
dnis-map            Entries    URL
--------            -------    ---
dmap1               1
*dmap4              0          http://dnismaps/dnismap4.txt
```

To create a DNIS map, use the **voice dnis-map** command. You can link to an external DNIS map text file or use the **dnis** command to add numbers to a DNIS map in Cisco IOS software.

To associate a DNIS map with a dial peer, use the **dnis-map** command.

Examples

The following is sample output from the **show voice dnis-map** command:

```
Router# show voice dnis-map

There are 2 dnis-maps configured

Dnis-map dmap1
---------------------------------------
  It has 3 entries
  It is not populated from a file.
```

```
DNIS                 URL
----                 ---
 4085551212          tftp://global/tickets/movies.vxml
 4085551234          tftp://global/tickets/plays.vxml
 4085554321          tftp://global/tickets/games.vxml


Dnis-map dmap4
---------------------------------------
  It has 0 entries
  It is populated from url http://dnismaps/dnismap4.txt


DNIS               URL
----               ---
```

Table 199 describes the fields shown in this output.

Table 199 show voice dnis-map Field Descriptions

Field	Description
Dnis-map	Name of a DNIS map that is configured on the gateway.
DNIS	Destination telephone number specified in this DNIS map.
URL	Location of the VoiceXML document to invoke for this DNIS number.

The following is sample output from the **show voice dnis-map summary** command:

```
Router# show voice dnis-map summary

There are 3 dnis-maps configured

dnis-map            Entries    URL
--------            -------    ---
dmap1               3
dmap4               0        http://dnismaps/dnismap4.txt
dmap6               8
```

Table 200 describes the fields shown in this output.

Table 200 show voice dnis-map summary Field Descriptions

Field	Description
dnis-map	Names of the DNIS maps that are configured on the gateway.
Entries	Number of entries in DNIS maps that reside on the gateway. This field displays 0 if the DNIS map is a text file stored on an external server.
URL	Location of externally stored DNIS maps.

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis-map	Associates a DNIS map to a dial peer.
voice dnis-map	Enters DNIS map configuration mode to create a DNIS map.
voice dnis-map load	Reloads a DNIS map that has changed since the previous load.

show voice dsmp stream

To display the current session of voice Distributed Stream Media Processor (DSPM) media stream, the recent state transitions, and stream connection, use the **show voice dsmp stream** command in privileged EXEC mode.

show voice dsmp stream {*stream ID* | **leg**}

Syntax Description

stream ID	DSMP media stream identifier. Range: 1 to 4294967295.
leg	Call leg corresponding to a caller ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When the calls hang, use this command to get the current sessions of the DSMP media stream. You can look at the DSMP state transitions corresponding to the calls and find out the problems.

Examples

The following example shows an output of a typical DSMP session in a VoIP call. This call consists of four streams, two input streams and two output streams:

```
Router# show voice dsmp stream
Total number of streams in use is: 4


Stream information:: stream=1
Type: TDM, Direction: OUTPUT
Fax/Modem Type: voice
Xmit Function: 0x00000000
Xmit function is Enabled
Call ID: 4, Conference ID: -1


Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367121.596 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367121.796 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.712 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.732 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.920 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
```

```
367122.940 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367123.112 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367123.152 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.432 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.632 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.732 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.932 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367125.032 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367125.232 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.140 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.160 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.340 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.380 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.548 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.568 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367122.652            4000    0x6113397C
            367119.388            4000    0x6113397C
            367117.624           10000    0x6112ED88

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367122.656               0    0x61133A98
            367119.392               0    0x61133A98
            367117.624               0    0x6112F060
            367117.624               0    0x6112EE24
    Number of overwritten entries: 2

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled


Stream information:: stream=3
Type: PACKET, Direction: OUTPUT
Fax/Modem Type: voice
Xmit Function: 0x6111D324
Xmit function is Enabled
Call ID: 3, Conference ID: 2
DSP Encap: 0x1
Codec Mask: 0x4; Codec Bytes: 20
Fax Rate Mask: 0x2; Fax Bytes: 20; T38 Disabled
```

```
VAD Mask: 0x2


Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367128.452 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367128.652 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.556 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.588 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.756 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.796 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.968 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.988 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.276 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.472 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.572 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.772 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.872 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367132.072 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367132.980 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.000 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.180 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.220 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.420 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
            367122.652            4000    0x6113397C
            367119.388            4000    0x6113397C
    Number of overwritten entries: 1

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
            367122.656               0    0x61133A98
```

```
            367119.392               0    0x61133A98
    Number of overwritten entries: 4

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled


Stream information:: stream=4
Type: PACKET, Direction: INPUT
Fax/Modem Type: voice
Xmit Function: 0x61F2CA34
Xmit function is Enabled
Call ID: 3, Conference ID: 2
DSP Encap: 0x1
Codec Mask: 0x4; Codec Bytes: 20
Fax Rate Mask: 0x2; Fax Bytes: 20; T38 Disabled
VAD Mask: 0x2


Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367133.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.420 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.692 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.892 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.992 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.192 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.292 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.492 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.432 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.600 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.640 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.812 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.840 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.112 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.312 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.412 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.612 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
```

```
367138.712 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.912 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367137.648            4000    0x6113397C
            367134.440            4000    0x6113397C
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
    Number of overwritten entries: 3

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367137.648               0    0x61133A98
            367134.440               0    0x61133A98
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
    Number of overwritten entries: 6

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled


Stream information:: stream=5
Type: TDM, Direction: INPUT
Fax/Modem Type: voice
Xmit Function: 0x00000000
Xmit function is Enabled
Call ID: 4, Conference ID: -1


Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367138.712 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.912 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367139.824 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367139.844 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.024 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.064 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.244 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.252 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367141.536 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367141.736 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
```

```
367141.836 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.036 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.136 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.336 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.244 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.264 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.444 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.484 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.652 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.672 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367137.648            4000    0x6113397C
            367134.440            4000    0x6113397C
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
    Number of overwritten entries: 3

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367137.648               0    0x61133A98
            367134.440               0    0x61133A98
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
    Number of overwritten entries: 6

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled
```

Table 201 describes the significant fields shown in the display.

Table 201 show voice dsmp stream Field Descriptions

Field	Description
Stream information	Shows stream ID.
Type	Type of stream.
Direction	Direction of stream.
Fax/Modem Type	Type of fax or modem.
Xmit Function	Transmit function in use.
Call ID	Caller ID of call leg.
Conference ID	Conference ID.

Table 201 show voice dsmp stream Field Descriptions (continued)

Field	Description
Session information	Information about the associated session.
connections	Number of stream connections.
streams	Number of streams.
current state	Current state and container of the session.
State Transitions	State transitions of the associated session.
DSP Encap	Encapsulation associated with the session.
Codec Mask	Codec mask associated with the session.
Fax Rate Mask	Fax rates associated with the session.
Fax Bytes	Fax bytes associated with the session.
VAD Mask	VAD mask associated with the session.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls in progress.
show voice call	Displays the call status for voice ports on the Cisco router.

show voice dsp

To display the current status or selective statistics of digital signal processor (DSP) voice channels, use the **show voice dsp** command in user EXEC or privileged EXEC mode.

show voice dsp [**active** [**slot** *slot-number* [*slot-number*]] | **capabilities slot** *slot-number* **dsp** *dsp-number* | **cpu-load slot** *slot-number* **dsp** *dsp-number* [**reset**] | **detailed** | **error** | [**group all** | **sorted-list**] **slot** *slot-number* | **signalling** | **voice** | **version** [*slot* | *slot*/*dsp*] [*slot* | *slot*/*dsp*]]

Cisco ASR 1000 Series Routers

show voice dsp [**active** [**slot** *slot-number*] | **capabilities slot** *slot-number* **dsp** *dsp-number* | **cpu-load slot** *slot-number* **dsp** *dsp-number* [**reset**] | **crash-dump** | **detailed** | **error** | **group** {**all** | **slot** *slot-number}* | **signalling** | **sorted-list slot** *slot-number* | **voice**]

Syntax Description

active	(Optional) Displays active channels.
slot *slot-number* [*slot-number*]	(Optional) Specifies either a single slot or the first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All slots in the range are affected by the command.
capabilities	(Optional) Displays DSP capabilities.
dsp *dsp-number*	(Optional) Specifies the DSP on the slot.
cpu-load	(Optional) Displays DSP CPU load.
reset	(Optional) Resets the DSP CPU statistics.
crash-dump	(Optional) Displays the DSP crash dump status. **Note** To enable a DSP crash dump, set file limit to a non-zero number, and set the destination to a valid file name.
detailed	(Optional) Displays detailed information about DSP status.
error	(Optional) Displays DSP errors.
group	(Optional) Displays DSP group information.
all	(Optional) Displays all the DSP group details.
sorted-list	(Optional) Displays a DSP sorted list.
signaling	(Optional) Displays DSP signaling channel usage.
voice	(Optional) Displays DSP voice channel usage.
version	(Optional) Displays the DSP firmware version.
slot	(Optional) The first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All slots in the range are affected by the command.
/dsp	(Optional) The first DSP in a range. To specify a range of DSPs, you can enter a second DSP in the syntax of this argument. The second DSP specifies the end of the range. All DSPs in the range are affected by the command. The slash mark is required.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series, and the display format was modified.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.3(14)T	The command was modified. Command output was enhanced to display status information for NM-HDV network module TI-549 DSPs.
12.4(4)T	The command was modified. Command output was enhanced to display the codec setting for modem relay operation.
12.4(4)XC	The command was modified. The **version** keyword was added and the command was implemented on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(11)T	The command was modified. Command output was enhanced to display information about DSP H.320 channels.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.2S	This command was implemented on the Cisco ASR 1000 Series Router.

Usage Guidelines

Use this command when abnormal behavior occurs in the DSP voice channels. The channel or channels should have an active voice call at the time the command is executed.

Examples

The following sample output shows the current status of the codec, set for modem relay, on channel 1:

```
Router# show voice dsp

----------------------------FLEX VOICE CARD 1 -------------------------------
                           *DSP VOICE CHANNELS*
DSP   DSP              DSPWARE CURR  BOOT                          PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 01 modem-re 4.5.909 busy  idle      0  0 1/1/0     05    0      298/353
                           *DSP SIGNALING CHANNELS*
DSP   DSP              DSPWARE CURR  BOOT                          PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 05 {flex}   4.5.909 alloc idle      0  0 1/1/3     02    0          15/0
C5510 001 06 {flex}   4.5.909 alloc idle      0  0 1/1/2     02    0          17/0
C5510 001 07 {flex}   4.5.909 alloc idle      0  0 1/1/1     06    0          31/0
C5510 001 08 {flex}   4.5.909 alloc idle      0  0 1/1/0     06    0         321/0
-----------------------END OF FLEX VOICE CARD 1 ----------------------------
```

The following sample output shows the current status of all DSP voice channels:

```
Router# show voice dsp

DSP# 0, channel# 0 G729A BUSY
DSP# 0, channel# 1 G729A BUSY
DSP# 1, channel# 2 FAX IDLE
DSP# 1, channel# 3 FAX IDLE
DSP# 2, channel# 4 NONE BAD
DSP# 2, channel# 5 NONE BAD
DSP# 3, channel# 6 NONE BAD
```

```
DSP# 3, channel# 7 NONE BAD
DSP# 4, channel# 8 NONE BAD
DSP# 4, channel# 9 NONE BAD
DSP# 5, channel# 10 NONE BAD
DSP# 5, channel# 11 NONE BAD
```

The following is sample output from this command on a Cisco 1750 router:

```
Router# show voice dsp

DSP#0: state IN SERVICE, 2 channels allocated
channel#0: voice port 1/0, codec G711 ulaw, state UP
channel#1: voice port 1/1, codec G711 ulaw, state UP
DSP#1: state IN SERVICE, 2 channels allocated
channel#0: voice port 2/0, codec G711 ulaw, state UP
channel#1: voice port 2/1, codec G711 ulaw, state UP
DSP#2: state RESET, 0 channels allocated
```

The following is sample output from this command on a secure Survivable Remote Site Telephony (SRST) router with the NM-HDV network module and the TI-549 (C549) DSP installed:

```
Router# show voice dsp

DSP  DSP    DSPWARE  CURR     BOOT                                  PAK   TX/RX
TYPE NUM CH CODEC    VERSION  STATE STATE  RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ======== === ==== ===========
C549  1  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   1   0    9357/9775
C549  1  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   2   0    0/0
C549  2  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   3   0    0/0
C549  2  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   4   0    0/0
C549  3  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   5   0    0/13
C549  3  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   6   0    0/13
```

The following is sample output from this command for an H.320 network configured for video support:

```
Router# show voice dsp

DSP  DSP             DSPWARE CURR  BOOT                          PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============ edsp 001
01 g711ulaw  0.1 IDLE  50/0/1.1 edsp 002 02 g711ulaw  0.1 IDLE  50/0/1.2 edsp 003 01
g729r8 p  0.1 IDLE  50/0/2.1 ----------------------------FLEX VOICE CARD 1
------------------------------
                        *DSP VOICE CHANNELS*
DSP   DSP             DSPWARE CURR  BOOT                           PAK   TX/RX
TYPE  NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 05 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 06 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 07 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 08 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 09 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 10 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 11 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 12 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 13 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 14 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 15 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 16 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 01 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 02 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 03 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 04 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 05 None     9.0.105 idle  idle      0  0                 0          0/0
```

```
C5510 003 06 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 07 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 08 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 09 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 10 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 11 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 12 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 13 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 14 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 15 None     9.0.105 idle  idle      0  0                  0          0/0
C5510 003 16 None     9.0.105 idle  idle      0  0                  0          0/0
                                  *DSP H.320 CHANNELS*
DSP   DSP     TX/RX       DSPWARE CURR               PAK   TX/RX
TYPE  NUM CH  CODEC       VERSION STATE VOICEPORT TS ABRT PACK COUNT
===== === === =========== ======= ===== ========= == ==== ============
C5510 001 01  h320p(01)   9.0.105 busy  1/0/0:15  06
      001 02  h320s(02)   9.0.105 busy  1/0/0:15  07
      001 03  h320s(03)   9.0.105 busy  1/0/0:15  08
      001 04  h320s(04)   9.0.105 busy  1/0/0:15  09
      001 01a g711ulaw    9.0.105 busy                0 1013663/5083
                                                                  00
      001 01v h263 /h263  9.0.105 busy                0 104908/30911
                                                                  4
------------------------END OF FLEX VOICE CARD 1 ----------------------------
```

Table 202 describes the significant fields shown in the displays.

Table 202 show voice dsp Field Descriptions

Field	Description
DSP	Number of the DSP.
channel	Number of the channel and its status.
DSP TYPE	TI-549 (C549) DSP.
DSP NUM	Number of the DSP.
CH	Channel number.
CODEC	Complexity setting.
DSPWARE VERSION	Version of DSPware.
CURR STATE	Current status of the channel: alloc (allocated), busy, or idle.
BOOT STATE	DSP readiness, either idle or in service.
RST	Number of times the DSP has been reset or restarted.
AI	Alarm indication count on the channel.
VOICEPORT	Voice card number and slot.
TS	Time slot.
PAK ABORT	Number of dropped packets.
TX/RX PACK COUNT	Number of transmitted and received packets.

Cisco ASR 1000 Series Router

The following sample output shows the DSP Type, DSP number, channel number, codecs running, DSP firmware version, and the current state of channels running on the DSP SPA inside the Cisco ASR 1000 Series Router:

```
Router# show voice dsp
---------------------------- SPA-DSP 1/1 ---------------------------

       *DSP INFORMATION*
DSP    DSP                DSPWARE CURR
TYPE   NUM CH CODEC       VERSION STATE RST AI
====== === == ========= ======== ===== === ==
SP2600 001    None       26.07.00 up    4   0
SP2600 002    None       26.07.00 up    3   0
SP2600 003    None       26.07.00 up    3   0
SP2600 004    None       26.07.00 up    1   0
SP2600 005    None       26.07.00 up    1   0
SP2600 006    None       26.07.00 up    1   0
SP2600 007    None       26.07.00 up    1   0
SP2600 008    None       26.07.00 up    1   0
SP2600 009    None       26.07.00 up    1   0
SP2600 010    None       26.07.00 up    1   0
SP2600 011    None       26.07.00 up    1   0
SP2600 012    None       26.07.00 up    1   0
SP2600 013    None       26.07.00 up    1   0
SP2600 014    None       26.07.00 up    1   0
SP2600 015    None       26.07.00 up    1   0
SP2600 016    None       26.07.00 up    1   0
SP2600 017    None       26.07.00 up    1   0
SP2600 018    None       26.07.00 up    1   0
SP2600 019    None       26.07.00 up    1   0
SP2600 020    None       26.07.00 up    1   0
SP2600 021    None       26.07.00 up    1   0

------------------------- END OF SPA-DSP 1/1 -----------------------------------
```

The following example shows the active channels on DSP SPA located in slot 1 on the Cisco ASR 1000 Series Router:

```
Router# show voice dsp active slot 1
------------------ SPA-DSP 1/1 ---------------------------
*DSP VOICE CHANNELS*
DSP    DSP                DSPWARE CURR
TYPE   NUM CH CODEC       VERSION STATE RST AI
====== === == ========= ======== ===== === ==
SP2600 001 01 g711ulaw  26.07.00 busy  4   0
SP2600 002 01 g711ulaw  26.07.00 busy  3   0
------------------------- END OF SPA-DSP 1/1 ------------
```

The following example shows the channel capabilities for different types of codecs on the Cisco ASR 1000 Series Router:

```
Router# show voice dsp capabilities slot 1

Card 1/1 DSP 1 Capabilities:
DSP Type: SP2600 - 43

    Credits   645 ,  G711Credits 15,  HC Credits  37,  MC Credits  23,
    FC Channel  43,  HC Channel  17,  MC Channel  28,
    Conference 8-party credits:
     G711  58 ,  G729  107,  G722  129,  ILBC  215
  Secure Credits:
```

```
    Sec LC Xcode  24,      Sec HC Xcode  64,
    Sec MC Xcode  35,      Sec G729 conf 161,
    Sec G722 conf 215,     Sec ILBC conf 322,
    Sec G711 conf 92 ,
  Max Conference Parties per DSP:
    G711 88,  G729 48,  G722 40,  ILBC 24,
    Sec G711 56,  Sec G729 32,
    Sec G722 24  Sec ILBC 16,
  Voice Channels:
    g711perdsp = 43,  g726perdsp = 28, g729perdsp = 17, g729aperdsp = 28,
    g723perdsp = 17,  g728perdsp = 17, g723perdsp = 17, gsmperdsp   = 28,
    gsmefrperdsp = 17, gsmamrnbperdsp = 17,
    ilbcperdsp = 17, isacperdsp = 8  modemrelayperdsp = 17,
    g72264Perdsp = 28, h324perdsp = 17,
    m_f_thruperdsp = 43, faxrelayperdsp = 28,
    maxchperdsp = 43, minchperdsp = 17,
    srtp_maxchperdsp = 27, srtp_minchperdsp = 14, faxrelay_srtp_perdsp =
4,
    g711_srtp_perdsp = 27, g729_srtp_perdsp = 14, g729a_srtp_perdsp = 24,----------
```

The following example shows the details of the DSP errors on the Cisco ASR 1000 Series Router.

Note The crash dump details must be enabled to display the crash dump for a DSP SPA. To enable a crash dump, set the destination of the crash dump file to a valid file name, and set the file limit to a non-zero number.

```
Router#show voice dsp crash-dump

Voice DSP Crash-dump status:
    Destination file url is <none>
    File limit is 0
DSP crash dump is currently disabled
To enable DSP crash dump, set file-limit to a non-zero number and set
destination to a valid file name
```

Related Commands

Command	Description
dsp services dspfarm	Enables the DSP-farm services.
dspfarm profile	Enters the DSP farm profile configuration mode and defines a profile for DSP farm services.
show dspfarm	Displays DSP farm service information, such as operational status, and DSP resource allocation for transcoding.

show voice dsp channel

To display the voice digital signal processor (DSP) channels, use the **show voice dsp channel** command in user EXEC or privileged EXEC mode.

show voice dsp channel {**operational-status** {*slot* | */dsp* | */channel*} [*slot* | */dsp* | */channel*] | **statistics** *slot-number* [*slot-number*] | **traffic** *slot-number* [*slot-number*]}

Syntax Description

operational-status	Displays the operational state for active sessions on a specific channel or range of channels.
slot	A single slot or the first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All slots in the range are affected by the command.
/dsp	A single DSP on the slot or the first DSP in a range. To specify a range of DSPs, you can enter a second DSP in the syntax of this argument. The second DSP specifies the end of the range. All DSPs in the range are affected by the command. The slash mark is required.
/channel	A single DSP channel or the first DSP channel in a range. The second occurrence of this argument specifies either a single DSP channel or the last DSP channel in a range. The slash mark is required.
statistics	Displays DSP statistics for a specific channel or range of channels.
slot-number	A single slot or the first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All slots in the range are affected by the command.
traffic	Displays traffic on a specific channel or range of channels.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	The command was introduced on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(11)T	The command was modified. Command output was enhanced to display information about DSP H.320 channels.

Usage Guidelines

Use this command when abnormal behavior occurs in the DSP voice channels. The channel or channels should have an active voice call at the time the command is executed.

Examples

The following is sample output from the **show voice dsp channel operational-status** command on slot 3/13/1:

```
Router# show voice dsp channel operational-status 3/13/1

 Operational status of Slot/DSP/Channel : 3/13/1
```

```
 Servicetype  : VOICE
 Codec Type  : gsmamr-nb
 Encapsulation : RTP
 Transmitted Packets : 346
 Transmitted Bytes : 11740
 Received Packets : 411
 Received Bytes : 11142
 Playout de-jitter mode :  None
 Playout de-jitter buffer minimum delay : 0 msec
 Playout de-jitter buffer initial delay : 0 msec
 Playout de-jitter buffer maximum delay : 0 msec
 Noise level : -5.0
 ERLLevel : 6
 ACOMLevel : 6
CodecPktPeriod=20 Milliseconds
CodecFrameFormat=bandwidth-efficient
CodecCrc=Disabled
CodecModes=3,6
CodecEncodeRate=6
CodecDecodeRate=6
CodecEncodeChanges=1
CodecDecodeChanges=0
CodecCrcFails=0
CodecBadFrameQuality=0
CodecInvalidCMRs=0
CodecInvalidFrameType=0
 Voice activity detection : Enabled
 Dtmf Relay : inband-voice
 ComfortNoisePak : 52
 TxVoiceDuration : 11560
 VoiceRxDuration : 3380
 Rx OutOfSeq Paks : 0
 Rx Late Paks : 0
 Rx Early Paks : 0
 Lost Packets : 0
 Playout Delay Current : 50
 Playout Delay Min : 50
 Playout Delay Max : 50
 Playout Delay ClockOffset : 80
 Playout Delay Jitter : 0
 Error Rx Drop : 0
 Error Tx Drop : 0
 Error Tx Control : 0
 Error Rx Control : 0
 Playout Error Predictive : 0
 Playout Error Interpolative : 0
 Playout Error Silence : 0
 Playout Error BufferOverFlow : 0
 Playout Error Retroactive : 0
 Playout Error Talkspurt : 0
```

Table 203 describes the significant fields shown in the display.

Table 203 show voice dsp channel Field Descriptions

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.
Codec Type	Complexity setting.
TxVoiceDuration	Transmitted voice duration.

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels,.

show voice dsp crash-dump

To display voice digital signal processor (DSP) crash dump information, use the **show voice dsp crash-dump** command in privileged EXEC configuration mode.

show voice dsp crash-dump

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example checks your configuration:

```
Router# show voice dsp crash-dump

Voice DSP Crash-dump status:
    Destination file url is slot0:banjo-152-s
    File limit is 20
    Last DSP dump file written was
          tftp://112.29.248.12/tester/26-152-t2
    Next DSP dump file written will be slot0:banjo-152-s1
```

The following example shows that the crash dump feature is enabled:

```
Router# show voice dsp crash-dump

Voice DSP Crash-dump status:
    Destination file url is
          tftp://172.29.248.12/xxtir/dspdump6.bin
    File limit is 10
    Last DSP dump file written was
          tftp://172.29.248.12/xxtir/dspdump6.bin1
    Next DSP dump file written will be
          tftp://172.29.248.12/xxtir/dspdump6.bin2
```

The following example shows that the crash dump feature is disabled:

```
Router# show voice dsp crash-dump

Voice DSP Crash-dump status:
    Destination file url is
          tftp://172.29.248.12/xxtir/dspdump6.bin
    File limit is 0
    Last DSP dump file written was
          tftp://172.29.248.12/xxtir/dspdump6.bin1
DSP crash dump is currently disabled
To enable DSP crash dump, set file-limit to a non-zero number
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug voice dsp crash-dump	Displays crash dump debug information.
voice dsp crash-dump	Enables the crash dump feature and specifies the destination file and the file limit.

show voice dsp summary

To display the digital signal processor (DSP) summary, use the **show voice dsp summary** command in user EXEC or privileged EXEC mode.

show voice dsp summary [*slot* | *slot*/*dsp*] [*slot* | *slot*/*dsp*]

Syntax Description

slot	(Optional) A single slot or the first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All slots in the range are affected by the command.
/dsp	(Optional) A single DSP on the slot or the first DSP in a range. To specify a range of DSPs, you can enter a second DSP in the syntax of this argument. The second DSP specifies the end of the range. All DSPs in the range are affected by the command. The slash mark is required.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	This command was introduced. The command was implemented on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(11)T	The command was modified. Command output was enhanced to display information about DSP H.320 channels.
12.4(19)	The command was modified. Command output was modified to accurately show the “Codectype” as “voice” rather than “fax” for T.38 calls.
12.4(18a)	The command was modified. Command output was modified to accurately show the “Codectype” as “voice” rather than “fax” for T.38 calls.
12.4(13f)	The command was modified. Command output was modified to accurately show the “Codectype” as “voice” rather than “fax” for T.38 calls.
12.4(15)T5	The command was modified. Command output was modified to accurately show the “Codectype” as “voice” rather than “fax” for T.38 calls.

Examples

The following sample output from the **show voice dsp summary** command shows summary information about DSPs:

```
Router# show voice dsp summary

Total number of DSPs = 48

Codectype       Calls    Codectype       Calls    Codectype       Calls
g729r8 pre-ietf     0    g729ar8             0    g726r16             0
g726r24             0    g726r32             0    g711ulaw            0
g711alaw            1    g728                0    g723r63             0
g723r53             0    gsmfr               0    gsmefr              0
g729br8             0    g729abr8            0    g723ar63            0
g723ar53            0    g729r8              0    t38                 0
clear-channel       0    vofr cisco          0    llcc                0
```

```
g726r40             0    transparent          0    modem-relay          0
cisco               0                         0                         0
pass-through        0    gsmamr-nb            0

Legend       :
======
Channel state: (s)shutdown    (a)active call (d)download pending
               (b)busiedout   (B)bad          (p)busyout pending
Call type    : (v)voice       (f)fax-relay    (_)not in use

Summary      :
=======
Channels     :  Total 768  In-Use    001
Calls        :  Total 001  Voice     001  Fax  000
             :  Free  713  Disabled  000

      DSP      DSP         DSP    Channel             Call
DSP#  State    Complexity  Resets State               Type
2/1   ACTIVE   FLEXI       0      _________ _________  _________ _________
2/2   ACTIVE   FLEXI       0      _________ _________  _________ _________
2/3   ACTIVE   FLEXI       0      _________ _________  _________ _________
2/4   ACTIVE   FLEXI       0      _________ _________  _________ _________
2/5   ACTIVE   FLEXI       0      _________ _________  _________ _________
2/6   ACTIVE   FLEXI       0      _________ _________  _________ __________
```

Table 202 describes the significant fields shown in the display.

Table 204 show voice dsp summary Field Descriptions

Field	Description
DSP	Number of the DSP.
Codectype	Complexity setting.
Channels	Number of the channel and its status.
State	Status of the calls.

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels,.

show voice eddri prefix

To show applicable prefixes for the event dispatcher and data repository interface (EDDRI), use the **show voice eddri prefix** command in privileged EXEC mode.

show voice eddri prefix [*prefix_number*]

Syntax Description

all	All neighbors
prefix_number	(Optional) Specified EDDRI prefix.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines If no prefix is specified, all configured prefixes appear.

The EDDRI notifies threaded grep (TGREP) when an attribute changes on some subsystems. EDDRI interacts with the dial-peer subsystem, trunk-group subsystems, call-control API (CCAPI) subsystem, and customer-relationship-management (CRM) subsystem to notify changes in particular attributes. EDDRI is responsible for creating the prefix database.

Examples The following example shows output for the **show voice eddri prefix** command:

```
prefix 4 address family decimal
advertise flag 0x27 ac 24 tc 24 capacity timer 25 sec
AC_avg 24, FD_avg 0, SD_avg 0
succ_curr 0 tot_curr 0
succ_report 0 tot_report 0
changed 0 replacement position 0
trunk group castg2
dial peer tag 1001
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug voip eddri	Turns on debugging for the EDDRI.

show voice enum-match-table

To display the rules of an ENUM match table, use the **show voice enum-match-table** command in privileged EXEC mode.

show voice enum-match-table [*table-number* [**sort**]]

Syntax Description

table-number	(Optional) ENUM match table to display, by number. Range is from 1 to 15.
sort	(Optional) Sorts the output by ascending table number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command displays the ENUM match table rules in the order in which they were defined. The **sort** keyword changes the display to list the rules from lowest to highest preference.

Examples

The following sample output displays the rules of ENUM match table number 3:

```
Router# show voice enum-match-table 3

voice enum_match_table 3
rule 1 5 /^9\(1.*\)/ /+\1/ cisco
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com
```

The following sample output displays the ENUM match tables in ascending order by table number:

```
Router# show voice enum-match-table

voice enum-match-table 3
rule 1 5 /^9\(1.*\)/ /+\1/ cisco
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com

voice enum-match-table 5
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
rule (ENUM configuration)	Defines the ENUM rule.
test enum	Tests the ENUM rule.
voice enum-match-table	Initiates the voice ENUM match table definition.

show voice hpi capture

To display capture status and statistics, use the **show voice hpi capture** command in privileged EXEC mode.

show voice hpi capture

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(10)	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command displays the capture status and statistics. Use this command to confirm logger status and to examine the logger status output when the logger is running.

Caution Using the message logger feature in a production network environment increases CPU and memory usage on the gateway.

Note If you are experiencing problems with certain voice calls, the engineering team at Cisco might ask you to capture the control messages using the voice DSP logger. You can capture these messages by turning on the logger, repeating the problematic calls, and capturing the logs. Only Cisco engineers can determine if you should send the logs in for further review.

Examples The following sample output shows capture statistics (HPI capture and logging) and status:

```
Router# show voice hpi capture

HPI Capture is on and is logging to URL ftp://172.23.184.216/d:\test_data.dat1 messages
sent to URL, 0 messages droppedMessage Buffer (total:inuse:free)  2134:0000:2134Buffer
Memory:699952 bytes, Message size:328 bytes
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug hpi	Enables debugging for HPI message events.
voice hpi capture	Allocates the Host Port Interface (HPI) capture buffer (size in bytes) and sets up or changes the destination URL for captured data.

show voice iec description

To display Internal Error Code (IEC) descriptions, use the **show voice iec description** command in user EXEC mode.

show voice iec description *string*

Syntax Description

string	Six-part dotted decimal string that displays the definition of an internal error code.

Command Default No default behavior or values.

Command Modes User EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example displays IEC descriptions:

```
Router# show voice iec description 1.1.180.2.21.4

    IEC Version: 1
    Entity: 1 (Gateway)
    Category: 180 (Software error)
    Subsystem: 2 (TCL IVR)
    Error: 21 (Script syntax)
    Diagnostic Code: 4
```

Table 205 describes significant fields shown in the display.

Table 205 show voice iec description Field Descriptions

Field	Description
IEC version	IEC version. A value of 1 indicates the Cisco IOS Release 12.3(4)T version.
Entity	Network physical entity (hardware system) that generated the IEC. The value 1 is assigned to the gateway.
Category	Error category, defined in terms of ITU-based Q.850 cause codes and VoIP network errors.
Subsystem	Specific subsystem within the physical entity where the IEC was generated.
Error Code	Error code within the subsystem.
Diagnostic Code	Cisco internal diagnostic value. Report this value to Cisco Technical Support.

Related Commands

Command	Description
show voice statistics iec	Displays IEC statistics.

show voice lmr

To display the Land Mobile Radio (LMR) related dynamic information and static information for LMR ports or a DS0 group, use the **show voice lmr** command in privileged EXEC mode.

show voice lmr [*slot*/*subunit*/*port* | *slot*/*port*:*ds0-group*] [**details** | **timing** [**warnings**]]

Syntax Description

slot/subunit/port	(Optional) Voice port that you specify with the *slot*/*subunit*/*port* designation. • *slot* specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. • *port* specifies an analog voice port number. Valid entries are 0 and 1. The slash marks are required.
slot/port:*ds0-group*	(Optional) Voice port that you specify with the *slot*/*port*:*ds0-group* designation. • *slot* specifies a router slot in which the packet voice NM is installed. Valid entries are router slot numbers for the particular platform. • *port* specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. • *ds0-group* specifies a T1 or E1 logical port number. T1 range is from 0 to 23. E1 range is from 0 to 30. The colon is required.
details	(Optional) Displays more information. If this keyword is omitted, less information is displayed.
timing	(Optional) Displays the timing configuration for all LMR ports.
warnings	(Optional) Displays all LMR ports that are having suspicious timing configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **timing** and **warnings** keywords were added.

Usage Guidelines

This command displays information for LMR voice ports only. If no voice port is specified, the command displays information for all ear and mouth (E&M) LMR voice ports.

When the **details** keyword is used, this command displays information about timeouts, timers, and injected tones and pauses, in addition to detailed voice port and active call information found in the **show voice port** and **show call active voice** commands.

Examples

The following is sample output from the **show voice lmr** command for an E&M LMR analog voice port on a Cisco 3745 router:

```
Router# show voice lmr 2/0/0

2/0/0
=========
 Connection type: n/a
 Out Attenuation = 0 db, In Gain = 0 dB
 E-lead capability is inactive, polarity = normal
 M-lead capability is inactive, polarity = normal
 voice-class tone-signal test
 state = LMR_CONNECT, e-lead = off, m-lead = off
 full duplex, voice path = rx
 Terminating side of the connection
 TransmitPackets=113, TransmitBytes=2241
 ReceivePackets=113, ReceiveBytes=2241
 CoderTypeRate=g729r8
 NoiseLevel=-65, ACOMLevel=22
 OutSignalLevel=-68, InSignalLevel=-79
 RemoteIPAddress=10.5.25.40, RemoteUDPPort=17272
 Remote SignallingIPAddress=10.5.25.40, Port=15418
 Remote MediaIPAddress=10.5.25.40, Port=17272
 RoundTripDelay=2 ms
 SessionProtocol=cisco
 VAD =enabled
```

The following is sample output from the **show voice lmr details** command for an E&M LMR analog voice port on a Cisco 3745 router:

```
Router# show voice lmr 2/0/0 details

2/0/0
=========
 Description:
 Connection type: n/a
 Out Attenuation = 0 db, In Gain = 0 dB
 Timing hangover: 500 ms
 E-lead capability is inactive, polarity = normal
 M-lead capability is inactive, polarity = normal
 Timing hookflash-in: 480
 Timing delay-voice: 470 ms
 Music On Hold Threshold: -38 dB, Noise Threshold: -62 dB
 E&M type: 1, Operation:  2-wire
 Impedance is set to 600r Ohm
 lmr tear down timeout is set to 1800 second
 lmr PTT transmit timeout is not set
 lmr PTT receive timeout is not set
 voice-class tone-signal test
         inject tone 1 1950 3 150
         inject tone 2 2000 0 60
         inject pause 3 60
         inject tone 4 2175 3 150
         inject tone 5 1000 0 50
         inject guard-tone 6 1950 -10
 state = LMR_CONNECT, e-lead = off, m-lead = off
 full duplex, voice path = rx
```

```
Terminating side of the connection
TransmitPackets=113, TransmitBytes=2241
ReceivePackets=113, ReceiveBytes=2241
CoderTypeRate=g729r8
NoiseLevel=-66, ACOMLevel=22
OutSignalLevel=-68, InSignalLevel=-79
PeerAddress=37200
PeerSubAddress=
PeerId=200
SessionTarget=

RemoteIPAddress=10.5.25.40, RemoteUDPPort=17272
Remote SignallingIPAddress=10.5.25.40, Port=15418
Remote MediaIPAddress=10.5.25.40, Port=17272
RoundTripDelay=0 ms
SessionProtocol=cisco
VAD =enabled
SelectedQoS=best-effort
ProtocolCallId=
SessionTarget=
```

Table 206 describes the significant fields shown in the output, in the order in which they appear.

Table 206 show voice lmr Field Descriptions

Field	Description
Connection type	Type of connection between LMR routers: private line, automatic ringdown (PLAR), trunk, or n/a
Out Attenuation	Output attenuation.
In Gain	Input gain.
E-lead capability	Active or inactive.
polarity	Polarity of the E&M voice port: normal or reverse.
M-lead capability	Active or inactive.
voice class tone-signal	Name of the tone-signal voice class.
state=	Signaling state.
e-lead =	On or off.
m-lead =	On or off.
full duplex	Voice path for the voice port is operating in full duplex mode.
half duplex	Voice path for the voice port is operating in half duplex mode.
voice path	Transmit or receive.
TransmitPackets	Number of packets sent by this peer during this call.
TransmitBytes	Number of bytes sent by this peer during this call.
ReceivePackets	Number of packets received by this peer during this call.
ReceiveBytes	Number of bytes received by the peer during this call.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.

Table 206 show voice lmr Field Descriptions (continued)

Field	Description
NoiseLevel	Active noise level for this call.
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceller, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
InSignalLevel	Active input signal level from the telephony interface used by this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
Remote SignallingIPAddress, Port	Call control server IP address and signaling port number.
Remote MediaIPAddress, Port	Remote side media server IP address and RTP port number.
RoundTripDelay	Voice packet round trip delay between the local and remote systems on the IP backbone for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
VAD	Whether voice activation detection (VAD) is enabled.
Description	Description of what the port is connected to.
Timing hangover	Number of milliseconds of delay before the digital signal processor (DSP) tells Cisco IOS software to turn off the E-lead after the DSP detects that the voice stream has stopped.
Timing hookflash-in	Maximum duration of a hookflash for a Foreign Exchange Station (FXS) interface.
Timing delay-voice	Delay before a voice packet is played out.
Music On Hold Threshold	Decibel level of music played when calls are put on hold.
Noise Threshold	Noise threshold for incoming calls.
E&M type	E&M signaling type.
Operation	2-wire or 4-wire operation.
Impedance	Terminating impedance of the interface.
lmr tear down timeout	Time for which the voice port waits before tearing down an LMR connection after detecting no voice activity.
lmr PTT transmit timeout	Maximum time for transmitting a voice packet.
lmr PTT receive timeout	Maximum time for receiving a voice packet.

Table 206 show voice lmr Field Descriptions (continued)

Field	Description
inject pause	Pause injected before the voice packet is played out.
inject tone	Tone injected before the voice packet is played out.
inject guard-tone	Guard tone played out with the voice packet.
PeerAddress	Destination pattern or number associated with this peer.
PeerSubAddress	Subaddress when this call is connected.
PeerId	ID value of the peer table entry to which this call was made.
SessionTarget	Network-specific address to receive calls from the dial peer.
SelectedQoS	Selected RSVP quality of service (QoS) for this call.
ProtocolCallId	Voice signaling specific call ID.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls in progress.
show voice port	Displays configuration information about a specific voice port.

show voice permanent-call

To display information about the permanent calls on a voice interface, use the **show voice permanent-call** command in user EXEC or privileged EXEC mode.

show voice permanent-call [*voice-port*] [**summary**]

Syntax Description

voice-port	(Optional) Slot number or slot/port number of the voice interface for which you wish to display permanent call information.
summary	(Optional) Displays summary information about VoFR and VoATM ports used for permanent connections.

Command Default

When no parameters are specified with this command, the output displays information for all ports containing permanent calls. When a specific interface is specified, information is displayed about the permanent calls for that interface only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	The command was integrated into Cisco IOS Release 12.0(4)T.

Examples

The following is sample output from the **show voice permanent-call** command:

```
Router# show voice permanent-call 1/1

1/1 state=connect coding=G729A payload size=30 vad=off
ec=8 (ms), cng=off fax=on digit_relay=on Seq num = off, VOFR Serial0,dlci = 550,cid = 6
TX INFO :slow-mode seq#= 25, sig pkt cnt= 19646, last-ABCD=1101
hardware-state ACTIVE signal type is CEPT/MELCAS
voice-gate CLOSED,network-path OPEN MASTER
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
RX INFO :slow-mode, sig pkt cnt= 19648, under-run = 0, over-run = 0
missing = 0, out of seq = 0, very late = 0
playout depth = 0 (ms), refill count = 1
 prev-seq#= 25, last-ABCD=1101, slave standby timeout 25000 (ms)
max inter-arrival time 0 (ms), current timer 384 (ms)
max timeout timer 5016 (ms), restart timeout is 0 (ms)
signaling packet fast-mode inter-arrival times (ms)
16 24 16 24 16 24 16 24 16 24 16 24 16 24 16 24
16 24 16 24 16 24 16 24 0 0 0 0 0 0 0 0
```

```
signaling playout history
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
```

The following is sample output from the **show voice permanent-call summary** command:

```
Router# show voice permanent-call summary

1/1 state= connect, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 880,cid = 6
1/2 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 102
1/3 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 103
1/4 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 104
1/5 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 105
1/6 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 106
1/7 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 107
1/8 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 108
1/9 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 109
1/10 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 110
1/11 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 111
1/12 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 112
1/13 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 113
1/14 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 114
1/15 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 115
1/17 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 117
1/18 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 118
1/19 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 119
1/20 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 120
1/21 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 121
1/22 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 122
1/23 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 123
1/24 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 124
1/25 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 125
```

Table 207 describes significant fields shown in this output.

Table 207 show voice permanent-call Field Descriptions

Field	Description
state	Current status of the call on this voice port.
coding	Codec type used for this call.
payload size	Size in bytes of the voice payload.
vad	Whether voice activity detection is turned on or off.
ec	Echo canceler length, in milliseconds.
cng	Whether comfort noise generation is used.
fax	Whether fax-relay is enabled.
digit_relay	Whether FRF.11 Annex A DTMF digit-relay is enabled.
Seq num	Whether sequence numbers are turned on or off.
VOFR	Interface used for this call.
dlci	DLCI for this call.
cid	DLCI subchannel for this call.
TX INFO:slow-mode	FRF.11 Annex B packets are being sent at the slow rate defined by the signal timing keepalive period.
TX INFO:seq#	Sequence number of the last packet sent.
TX INFO:sig pkt cnt	Number of signaling packets sent by this dial peer.
TX INFO:last-ABCD	Last ABCD signaling state sent by this dial peer to the network.
hardware-state	On-hook/off-hook state of the call when the signaling protocol in use is a supported protocol. Not valid when the signal type is “transparent.”
signal type	Type of call-control signaling used by this dial peer.
voice-gate	Whether voice packets are being sent (OPEN) or not sent (CLOSED).
network-path	Whether any type of packet is being sent (OPEN) or not sent (CLOSED) to the network. This field indicates CLOSED only if the port is configured as a slave using the **connection trunk answer-mode** command.
RX INFO:slow-mode	FRF.11 Annex B packets are being received at the slow rate. Successive packets have the same sequence number.
RX INFO:sig pkt cnt	Number of slow-mode signaling packets received by this dial peer.
RX INFO:under-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became empty during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.
RX INFO:over-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became full during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.
RX INFO:missing	Number of FRF.11 Annex B packets that were counted as missing based on checking Annex B sequence numbers.

Table 207 show voice permanent-call Field Descriptions (continued)

Field	Description
RX INFO:out of seq	Number of FRF.11 Annex B packets that were counted as received in the wrong order based on checking Annex B sequence numbers.
RX INFO:very late	Number of FRF.11 Annex B packets that were received with a sequence number significantly different from the expected sequence number.
RX INFO:playout depth	Valid for fast-mode only. Shows the current FRF.11 Annex B signaling buffer playout depth in milliseconds.
RX INFO:refill count	Indicates the number of times the FRF.11 Annex B signaling playout buffer was refilled as a result of a slow-mode to fast-mode transition.
RX INFO:prev-seq#	Sequence number of the last FRF.11 Annex B signaling packet received.
RX INFO:last-ABCD	Last ABCD signaling bit pattern sent to the attached PBX (telephone network side). In the out-of-service condition, this shows the OOS pattern being sent to the PBX.
RX INFO:slave standby timeout	Value configured using the **signal timing oos standby** command for the applicable voice class permanent entry.
max inter-arrival time	Maximum interval between the arrival of fast-mode FRF.11 Annex B packets since the last time this parameter was displayed.
current timer	Time, in milliseconds, since the last signaling packet was received.
max timeout timer	Maximum value of the “current timer” parameter since the last time it was displayed.
restart timeout	Connection restart timeout value.
signaling packet fast-mode inter-arrival time	Last several values of the fast-mode FRF.11 Annex B signaling packet inter-arrival time.
signaling playout history	Recent ABCD signaling bits received from the data network.

Related Commands

Command	Description
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.

show voice port

To display configuration information about a specific voice port, use the **show voice port** command in privileged EXEC mode.

Cisco 1750 Router

show voice port *slot/port*

Cisco 2600 and Cisco 3600 Series Router with Analog Voice Ports

show voice port [*slot/subunit/port* | **summary**]

Cisco 2600 and Cisco 3600 Series Router with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

show voice port [*slot/port*:*ds0-group* | **summary**]

Cisco AS5300 Universal Access Server

show voice port *controller-number*:**D**

Cisco 7200 Series Router

show voice port {*slot/port*:*ds0-group-number* | *slot/subunit/port*}

Syntax Description

Cisco 1750 Router	
slot	Slot number in the router in which the VIC is installed. Valid entries are 0, 1, and 2, depending on the slot in which it is installed.
/port	Voice port. Valid entries are 0 and 1. The slash mark is required.

Cisco 2600 and Cisco 3600 Series Router with Analog Voice Ports	
slot/subunit/port	(Optional) The analog voice port designation: • *slot*—Router slot in which a voice network module (VNM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit*—Voice Interface Card (VIC) in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) The slash mark is required. • *port*—Analog voice port number. Valid entries are 0 and 1. The slash mark is required.
summary	(Optional) Displays a summary of all voice ports.

Cisco 2600 and Cisco 3600 Series Router with Digital Voice Ports	
slot/*port*:*ds0-group*	(Optional) Specifies the digital voice port designation: • *slot*—Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • /*port*—T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • :*ds0-group*—T1 or E1 logical port number. T1 range is 0 to 23. E1 range is 0 to 30. The colon is required.
summary	(Optional) Displays a summary of all voice ports.

Cisco AS5300 Universal Access Server	
controller-number	T1 or E1 controller.
:D	D channel that is associated with the ISDN PRI. The colon is required.

Cisco 7200 Series Router	
slot	Router location where the voice port adapter is installed. Range is 0 to 3.
/*port*	Voice interface card location. Valid entries are 0 and 1. The slash mark is required.
:*ds0-group-number*	Defined DS0 group number. Because each defined DS0 group number is represented on a separate voice port, you can define individual DS0s on the digital T1/E1 card. The colon is required.
slot	Slot number in the Cisco router where the VIC is installed. Range is 0 to 3, depending on the slot where it is installed.
/*subunit*	Subunit on the VIC where the voice port is located. Valid entries are 0 and 1. The slash mark is required.
/*port*	Voice port number. Valid entries are 0 and 1. The slash mark is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was modified. Port-specific values for the Cisco MC3810 were added.
12.0(3)T	This command was modified. Port-specific values for the Cisco MC3810 were added.
12.0(5)XK	This command was modified. The *ds0-group* argument was added for the Cisco 2600 series and Cisco 3600 series.

Release	Modification
12.0(5)XE	This command was modified. Additional syntax was created for digital voice to allow specification of the DS0 group. This command applies to VoIP on the Cisco 7200 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was modified. The **summary** keyword was added for the Cisco 2600 series and Cisco 3600 series. The *ds0-group* argument was added for the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was modified. This command was implemented for direct inward dial (DID) on the Cisco IAD2420 series.
12.2(2)XN	This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. It was implemented on the Cisco IAD2420 series.
12.4(11)T	This command was modified. This command was enhanced to display voice class called-number-pool configuration information for the voice port.
12.4(12)	This command was modified. This command was integrated into Cisco IOS Release 12.4(12) and output was modified to display the parameter set by the **timing sup-disconnect** command.
15.0(1)XA	This command was modified. The output was enhanced to display the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The output of this command was enhanced to display the connection status of foreign exchange office (FXO) ports.

Usage Guidelines

Use this command to display configuration and VIC-specific information about a specific port.

This command works on Voice over IP, Voice over Frame Relay, and Voice over ATM.

The **ds0-group** command automatically creates a logical voice port that is numbered as follows on Cisco 2600, Cisco 3600 series, and Cisco 7200 series routers: *slot*/*port*:*ds0-group-number*. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Note This command is not supported on Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms for Non-Facility Associated Signaling (NFAS) configuration.

Examples

The following is sample output from the **show voice port** command for an E&M analog voice port:

```
Router# show voice port 1/0/0

E&M Slot is 1, Sub-unit is 0, Port is 0
 Type of VoicePort is E&M
 Operation State is unknown
 Administrative State is unknown
```

```
 The Interface Down Failure Cause is 0
 Alias is NULL
 Noise Regeneration is disabled
 Non Linear Processing is disabled
 Music On Hold Threshold is Set to 0 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is disabled
 Echo Cancel Coverage is set to 16ms
 Connection Mode is Normal
 Connection Number is not set
 Initial Time Out is set to 0 s
 Interdigit Time Out is set to 0 s
 Analog Info Follows:
 Region Tone is set for northamerica
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0

 Voice card specific Info Follows:
 Signal Type is wink-start
 Operation Type is 2-wire
 Impedance is set to 600r Ohm
 E&M Type is unknown
 Dial Type is dtmf
 In Seizure is inactive
 Out Seizure is inactive
 Digit Duration Timing is set to 0 ms
 InterDigit Duration Timing is set to 0 ms
 Pulse Rate Timing is set to 0 pulses/second
 InterDigit Pulse Duration Timing is set to 0 ms
 Clear Wait Duration Timing is set to 0 ms
 Wink Wait Duration Timing is set to 0 ms
 Wink Duration Timing is set to 0 ms
 Delay Start Timing is set to 0 ms
 Delay Duration Timing is set to 0 ms
```

The following is sample output from the **show voice port** command for an E&M digital voice port:

```
Router# show voice port 1/0/1

receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

The following is sample output from the **show voice port** command for a foreign exchange station (FXS) analog voice port:

```
Router# show voice port 1/1/1
```

```
Foreign Exchange Station 1/1/1 Slot is 1, Sub-unit is 1, Port is 1
 Type of VoicePort is FXS  VIC2-2FXS
 Operation State is DORMANT
 Administrative State is UP
 The Last Interface Down Failure Cause is Administrative Shutdown
 Description is I am a FXS LoopStart port
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Supervisory Disconnect Time Out is set to 750 ms
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US

 Analog Info Follows:
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Impedance is set to 600r Ohm
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):
 lpcor (Incoming): local_group
 lpcor (Outgoing): local_group

 Voice card specific Info Follows:
 Signal Type is loopStart
 Ring Frequency is 25 Hz
 Hook Status is On Hook
 Ring Active Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is active
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Hookflash-in Timing is set to max=1000 ms, min=150 ms
 Hookflash-out Timing is set to 400 ms
 No disconnect acknowledge
 Ring Cadence is defined by CPTone Selection
 Ring Cadence are [20 40] * 100 msec
 Ringer Equivalence Number is set to 1
```

The following is sample output from the **show voice port** command for an FXO analog voice port:

```
Router# show voice port 1/0/1

Foreign Exchange Office 1/0/1 Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 The Last Interface Down Failure Cause is Administrative Shutdown
 Description is I am an FXO LoopStart port
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US

 Analog Info Follows:
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Impedance is set to 600r Ohm
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):

 Voice card specific Info Follows:
 Signal Type is loopStart
 Battery-Reversal is enabled
 Number Of Rings is set to 1
 Supervisory Disconnect is signal
 Answer Supervision is inactive
 Hook Status is On Hook
 Ring Detect Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is inactive
 Dial Out Type is dtmf
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Pulse Rate Timing is set to 10 pulses/second
 InterDigit Pulse Duration Timing is set to 750 ms
 Percent Break of Pulse is 60 percent
 GuardOut timer is 2000 ms
 Minimum ring duration timer is 125 ms
 Hookflash-in Timing is set to 600 ms
 Hookflash-out Timing is set to 400 ms
```

```
 Supervisory Disconnect Timing (loopStart only) is set to 750 ms
 OPX Ring Wait Timing is set to 6000 ms
```

The following is sample output from the **show voice port summary** command. Note that for the connected FXO analog voice port 0/2/0, which has the ADMIN state of "up" and the OPER state of "dorm," this output shows that the IN STATUS is "idle" and the OUT STATUS is "on-hook":

```
Router# show voice port summary
                                          IN       OUT
PORT            CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
=============== == ============ ===== ==== ======== ======== ==
0/0/0           --  fxs-ls      up    dorm on-hook  idle     y
0/0/1           --  fxs-ls      up    dorm on-hook  idle     y
0/3/0:23        01  isdn-voice  up    dorm none     none     y
0/3/0:23        02  isdn-voice  up    dorm none     none     y
.
.
.
0/1/0           --  did-in-wnk  up    dorm idle     idle     y
0/1/1           --  did-in-wnk  up    dorm idle     idle     y
0/2/0           --  fxo-ls      up    dorm idle     on-hook  y
0/2/1           --  fxo-ls      up    down idle     off-hook y
2/0/0           --  fxs-ls      up    dorm on-hook  idle     y
2/0/1           --  fxs-ls      up    dorm on-hook  idle     y
2/0/2           --  fxs-ls      up    dorm on-hook  idle     y
2/0/3           --  fxs-ls      up    dorm on-hook  idle     y
2/0/4           --  fxs-ls      up    dorm on-hook  idle     y
2/0/5           --  fxs-ls      up    dorm on-hook  idle     y
2/0/6           --  fxs-ls      up    dorm on-hook  idle     y
2/0/7           --  fxs-ls      up    dorm on-hook  idle     y
```

Note If the FXO port 0/2/0 is disconnected, the output of the **show voice port summary** command changes so that the OUT STATUS is reported as "off-hook," and the OPER state changes to "down."

The following is sample output from the **show voice port** command for an ISDN voice port:

```
Router# show voice port

ISDN 2/0:23 Slot is 2, Sub-unit is 0, Port is 23
 Type of VoicePort is ISDN-VOICE
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
```

```
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):
 Voice class called number pool:

DS0 channel specific status info:
                                      IN      OUT
    PORT       CH  SIG-TYPE    OPER STATUS    STATUS    TIP     RING
    2/0:23     01  isdn-voice  up   none      none
    2/0:23     02  isdn-voice  up   none      none
    2/0:23     03  isdn-voice  up   none      none
    2/0:23     04  isdn-voice  up   none      none
    2/0:23     05  isdn-voice  up   none      none
    2/0:23     06  isdn-voice  up   none      none
    2/0:23     07  isdn-voice  dorm none      none
    2/0:23     08  isdn-voice  dorm none      none
    2/0:23     09  isdn-voice  dorm none      none
    2/0:23     10  isdn-voice  dorm none      none
    2/0:23     11  isdn-voice  dorm none      none
    2/0:23     12  isdn-voice  dorm none      none
    2/0:23     13  isdn-voice  dorm none      none
    2/0:23     14  isdn-voice  dorm none      none
    2/0:23     15  isdn-voice  dorm none      none
    2/0:23     16  isdn-voice  dorm none      none
    2/0:23     17  isdn-voice  dorm none      none
    2/0:23     18  isdn-voice  dorm none      none
    2/0:23     19  isdn-voice  dorm none      none
    2/0:23     20  isdn-voice  dorm none      none
    2/0:23     21  isdn-voice  dorm none      none
    2/0:23     22  isdn-voice  dorm none      none
    2/0:23     23  isdn-voice  dorm none      none
```

The following is sample output from the **show voice port** command for the connected FXO analog voice port 0/2/0, which has the Administrative State of “UP” and the Operation State of “DORMANT”:

```
Router# show voice port 0/2/0

Foreign Exchange Office 0/2/0 Slot is 0, Sub-unit is 2, Port is 0
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 128 ms
 Echo Cancel worst case ERL is set to 6 dB
```

```
Playout-delay Mode is set to adaptive
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Playout-delay Fax is set to 300 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 15 s
Interdigit Time Out is set to 10 s
Call Disconnect Time Out is set to 60 s
Power Denial Disconnect Time Out is set to 1000 ms
Ringing Time Out is set to 180 s
Wait Release Time Out is set to 30 s
Companding Type is u-law
Region Tone is set for US

Analog Info Follows:
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Station name None, Station number None
Translation profile (Incoming):
Translation profile (Outgoing):
lpcor (Incoming):
lpcor (Outgoing):

Voice card specific Info Follows:
Signal Type is loopStart
Battery-Reversal is enabled
Number Of Rings is set to 1
Supervisory Disconnect is signal
Answer Supervision is inactive
Hook Status is On Hook
Ring Detect Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Dial Out Type is dtmf
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Pulse Rate Timing is set to 10 pulses/second
InterDigit Pulse Duration Timing is set to 750 ms
Percent Break of Pulse is 60 percent
GuardOut timer is 2000 ms
Minimum ring duration timer is 125 ms
Hookflash-in Timing is set to 600 ms
Hookflash-out Timing is set to 400 ms
Supervisory Disconnect Timing (loopStart only) is set to 350 ms
OPX Ring Wait Timing is set to 6000 ms
Secondary dialtone is disabled
```

Note If the FXO port 0/2/0 is disconnected, the output of the **show voice port** command changes so that the Administrative State remains "UP" but the Operation State is "DOWN."

Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports—any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to "up" for FXO port 0/2/0:

```
000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0,
changed state to operational status up due to cable reconnection
```

Table 208 describes significant fields shown in these outputs, in alphabetical order.

Table 208 show voice port Field Descriptions

Field	Description
Administrative State	Administrative state of the voice port.
Alias	User-supplied alias for the voice port.
Clear Wait Duration Timing	Time (in milliseconds [ms]) of inactive seizure signal to declare call cleared.
Companding Type	Companding standard used to convert between analog and digital signals in pulse code modulation (PCM) systems.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or private line automatic ringdown (PLAR) mode.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Delay Duration Timing	Maximum delay signal duration (in ms) for delay dial signaling.
Delay Start Timing	Timing (in ms) of generation of delayed start signal from detection of incoming seizure.
Dial Type	Out-dialing type of the voice port.
Digit Duration Timing	Dual-tone multifrequency (DTMF) digit duration (in ms).
E&M Type	Type of E&M interface.
Echo Cancel Coverage	Echo cancel coverage for this port.
Echo Cancellation	Whether echo cancellation is enabled for this port.
Impedance	Configured terminating impedance for the E&M interface.
In Gain	Amount of gain (in decibels [dB]) inserted at the receiver side of the interface.
In Seizure	Incoming seizure state of the E&M interface.
Initial Time Out	Amount of time (in seconds) the system waits for an initial input digit from the caller.
Interdigit Duration Timing	DTMF interdigit duration (in seconds).
InterDigit Pulse Duration Timing	Pulse dialing interdigit timing (in ms).

Table 208 show voice port Field Descriptions (continued)

Field	Description
Interdigit Time Out	Amount of time (in seconds) the system waits for a subsequent input digit from the caller.
Lpcor (Incoming)	Setting of the **lpcor incoming** command.
Lpcor (Outgoing)	Setting of the **lpcor outgoing** command.
Maintenance Mode	Maintenance mode of the voice port.
Music On Hold Threshold	Configured music-on-hold threshold value for this interface.
Noise Regeneration	Whether background noise should be played to fill silent gaps if voice activity detection (VAD) is activated.
Non Linear Processing	Whether nonlinear processing is enabled for this port.
Number of signaling protocol errors	Number of signaling protocol errors.
Operation State	Operational state of the voice port.
Operation Type	Operation type of the E&M signal: 2-wire or 4-wire.
Out Attenuation	Amount of attenuation (in dB) inserted at the transmit side of the interface.
Out Seizure	Outgoing seizure state of the E&M interface.
Port	Port number for the interface associated with the voice interface card.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Region Tone	Configured regional tone for this interface.
Ring Active Status	Ring active indication.
Ring Cadence	Configured ring cadence for this interface.
Ring Frequency	Configured ring frequency (in hertz) for this interface.
Ring Ground Status	Ring ground indication.
Ringing Time Out	Ringing timeout duration (in seconds).
Signal Type	Type of signaling for a voice port: delay-dial, ground-start, immediate, loop-start, and wink-start.
Slot	Slot used in the voice interface card for this port.
Sub-unit	Subunit used in the voice interface card for this port.
Tip Ground Status	Tip ground indication.
Type of VoicePort	Type of voice port: FXO, FXS, or E&M.
The Interface Down Failure Cause	Text string describing why the interface is down,
Wait Release Time Out	Length of time (in seconds) that a voice port stays in call-failure state while a busy tone, reorder tone, or out-of-service tone is sent to the port.
Wink Duration Timing	Maximum wink duration (in ms) for wink-start signaling.
Wink Wait Duration Timing	Maximum wink wait duration (in ms) for wink-start signaling.

Related Commands

Command	Description
ds0 group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router communicates with the PBX or PSTN.
timing sup-disconnect	Defines the minimum time to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX).

show voice source-group

To display the details of one or more voice source IP groups, use the **show voice source-group** command in privileged EXEC mode.

show voice source-group [*name* | **sort** [**ascending** | **descending**]]

Syntax Description

name	(Optional) Name of the source IP group to display.
sort [**ascending** | **descending**]	(Optional) Displays the source IP groups in either ascending or descending alphanumerical order.

Command Default Ascending order

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples The following sample output shows an invalid configuration.

```
Router# show voice source-group abc

Source Group: abc
    description="",
    carrier-id source="sj_area",
    carrier-id target="",
    trunk-group-label source="",
    trunk-group-label target="ny_main",
    h323zone-id="",
    access-list=,
    disconnect-cause="no-service",
    translation-profile="",
```

The following sample output shows a valid configuration for carrier-ID routing:

```
Router# show voice source-group abc

Source Group: abc
    description="",
    carrier-id source="",
    carrier-id target="",
    trunk-group-label source="texas_backup",
    trunk-group-label target="ny_main",
    h323zone-id="",
    access-list=,
    disconnect-cause="no-service",
    translation-profile="",
```

If you are using carrier-ID routing, both carrier-ID fields are filled in and the "trunk-group-label" fields are blank.

The following sample output displays the source groups in ascending order. Both source IP groups use carrier-ID routing.

```
Router# show voice source-group sort ascending

Source Group:1
        description="routec calls from 1311 to 1411",
        carrier-id source="1311",
        carrier-id target="1411",
        trunk-group-label source="",
        trunk-group-label target="",
        h323zone-id="fr1311",
        access-list= ,
        disconnect-cause="user-busy",
        destination-pattern="",
        incoming called-number="",
        translation-profile="10",

Source Group:2
        description="",
        carrier-id source="abcd",
        carrier-id target="xyz",
        trunk-group-label source="",
        trunk-group-label target="",
        h323zone-id="",
        access-list= ,
        disconnect-cause="no-service",
        destination-pattern="",
        incoming called-number="",
        translation-profile="",
```

Table 209 describes significant fields shown in this output.

Table 209 show voice source-group Field Descriptions

Field	Description
Source Group	Name of the voice source IP group.
description	Description of the voice source IP group.
carrier-id source	Name of the source carrier ID used by the terminating gateway to select a target carrier.
carrier-id target	Name of the target carrier ID used by the terminating gateway to select a dial peer for routing the call over a POTS line.
trunk-group-label source	Name of the source trunk group used by the originating gateway to route the call over an inbound dial peer.
trunk-group-label target	Name of the target trunk group used by the terminating gateway to select a dial peer for routing an outbound call over a POTS line.
h323zone-id	Name of the zone associated with incoming H.323 calls to the voice source IP group.
access-list	Number of the access list used by the voice source IP group to block calls.
disconnect-cause	Phrase returned by the voice source IP group when a call is blocked.
translation-profile	Name of the translation profile used by the voice source IP group to translate calls.

Related Commands

Command	Description
voice source-group	Initiates a voice source IP group definition.

show voice statistics csr interval accounting

To display accounting statistics by configured intervals, use the **show voice statistics csr interval accounting** command in privileged EXEC mode.

show voice statistics csr interval tag-number accounting {**all** | **method-list** *method-list-name*} [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

tag-number	Interval that represents a specified time range. The valid range is from 1 to 36655. **Note** You must first enter the **show voice statistics interval-tag** command to obtain the valid tag numbers that you can enter for this command.
all	Displays all voice accounting statistics.
method-list-name *method-list-name*	Displays accounting statistics by method list. You must specify a method-list name.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • **all**—Pushes statistics to both the FTP and syslog servers. • **ftp**—Pushes statistics to the FTP server. • **syslog**—Pushes statistics to the syslog server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following sample output shows all of the statistics that were collected for interval tag 102 for method list h323-1:

```
Router# show voice statistics csr interval 102 accounting method-list h323-1

Client Type: Voice ACCT Stats
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:29Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=0,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=0
```

Table 210 lists and describes the significant output fields.

Table 210 show voice statistics csr interval accounting Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
method-list	The method list name.
acc_pass_criteria	Accounting pass criteria: • 1: all start/interim/stop messages passed. • 2: all start/stop messages passed. • 3: stop-only message passed.
pstn_in_pass	Number of incoming calls on the PSTN leg that meet acc_pass_criteria.
pstn_in_fail	Number of incoming calls on the PSTN leg that fail acc_pass_criteria.
pstn_out_pass	Number of outgoing calls on the PSTN leg that meet acc_pass_criteria.
pstn_out_fail	Number of outgoing calls on the PSTN leg that fail acc_pass_criteria.
ip_in_pass	Number of incoming calls on the IP leg that meet acc_pass_criteria.
ip_in_fail	Number of incoming calls on the IP leg that fail acc_pass_criteria.
ip_out_pass	Number of outgoing calls on the IP leg that meet acc_pass_criteria.
ip_out_fail	Number of outgoing calls on the IP leg that fail acc_pass_criteria.

Related Commands

Command	Description
show event-manager consumers	Displays event-manager statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics csr interval aggregation

To display signaling statistics by configured intervals, use the **show voice statistics csr interval aggregation** command in privileged EXEC mode.

show voice statistics csr interval tag-number aggregation {**all** | **gateway** | **ip** | **pstn** | **trunk-group** {*trunk-group-label* | **all** } | **voice-port** {*voice-port-label* | **all**}} [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

tag-number	Interval that represents a specified time range. The valid range is from 1 to 36655. **Note** You must first enter the **show voice statistics interval-tag** command to obtain the valid tag numbers that you can enter for this command.
all	Displays all levels of signaling statistics.
gateway	Displays gateway-wide level statistics.
ip	Displays VoIP interface level statistics.
pstn	Displays telephone interface level statistics.
trunk-group	Displays trunk-group level statistics. • *trunk-group-label*—displays statistics for a specific trunk group • **all**—Displays statistics for all trunk groups.
voice-port	Displays voice-port level statistics: • *voice-port-label*—displays statistics for a specific voice port • **all**—Displays statistics for all voice ports.
mode	(Optional) Statistics are displayed in a specified mode. The keywords are as follows: • **concise**—Displays output that contains total calls, answered calls, and answered call duration. • **verbose**—Displays all fields contained in call statistic records (CSRs). This is the default setting.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • **all**—Pushes statistics to both the FTP and syslog servers. • **ftp**—Pushes statistics to the FTP server. • **syslog**—Pushes statistics to the syslog server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command is valid only if the **voice statistics time-range** command is configured to either the **periodic** or **start-stop** value. If you enter the **show voice statistics csr interval aggregation** command but the gateway has been configured to collect statistics only since the last reset, the gateway displays an error message.

You must first enter the **show voice statistics interval-tag** to obtain the valid tag numbers that you can enter for this command.

Examples

The following sample output shows signaling statistics for all aggregation levels for interval tag 200:

```
Router# show voice statistics csr interval 200 aggregation all

Client Type: VCSR
        Start Time: 2002-04-28T01:48:24Z        End Time: 2002-04-28T01:50:01Z

record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
,out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

Table 211 lists and describes the significant output fields.

Table 211 show voice statistics csr interval aggregation Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than “normal”.
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than “normal”.
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.

Table 211 show voice statistics csr interval aggregation Field Descriptions (continued)

Field	Description
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies the time range to collect CSRs.

show voice statistics csr since-reset accounting

To display VoIP AAA accounting statistics since the last reset, use the **show voice statistics csr since-reset accounting** command in privileged EXEC mode.

show voice statistics csr since-reset accounting {**all** | **method-list** *method-list-name*} [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

all	All collected statistics since the last reset are displayed.
method-list *method-list-name*	Collected statistics by method list since the last reset are displayed. The *method-list-name* argument specifies the name of the method list.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • **all**—Pushes statistics to both the FTP and syslog servers. • **ftp**—Pushes statistics to the FTP server. • **syslog**—Pushes statistics to the syslog server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command only applies if the **voice statistics time-range** command is configured to the **since-reset** value. Voice statistics collection on the gateway is reset using the **clear voice statistics csr** command.

If you enter the **show voice statistics csr since-reset accounting** command but the gateway has been configured for periodic collection or to a specific interval, the gateway will display an error message.

Examples

The following sample output shows the accounting statistics for method list h323-1 since the last reset:

```
Router# show voice statistics csr since-reset accounting method-list h323-1

Client Type: Voice ACCT Stats
        Start Time: 2002-05-05T17:39:17Z        End Time: 2002-05-09T19:00:16Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=1,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=1
```

Table 212 lists and describes the significant output fields.

Table 212 show voice statistics csr since-reset accounting Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.

Table 212 show voice statistics csr since-reset accounting Field Descriptions (continued)

Field	Description
End Time	The ending time of the statistics collection.
method-list	The method list name.
acc_pass_criteria	Accounting pass criteria: • 1: all start/interim/stop messages passed. • 2: all start/stop messages passed. • 3: stop-only message passed.
pstn_in_pass	Number of incoming calls on the PSTN leg that meet acc_pass_criteria.
pstn_in_fail	Number of incoming calls on the PSTN leg that fail acc_pass_criteria.
pstn_out_pass	Number of outgoing calls on the PSTN leg that meet acc_pass_criteria.
pstn_out_fail	Number of outgoing calls on the PSTN leg that fail acc_pass_criteria.
ip_in_pass	Number of incoming calls on the IP leg that meet acc_pass_criteria.
ip_in_fail	Number of incoming calls on the IP leg that fail acc_pass_criteria.
ip_out_pass	Number of outgoing calls on the IP leg that meet acc_pass_criteria.
ip_out_fail	Number of outgoing calls on the IP leg that fail acc_pass_criteria.

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies a time range to collect statistics from the gateway on a periodic basis, since the last reset, or for a specific time duration.

show voice statistics csr since-reset aggregation-level

To display signaling statistics since the last reset, use the **show voice statistics csr since-reset aggregation-level** command in privileged EXEC mode.

show voice statistics csr since-reset aggregation-level {**all** | **gateway** | **ip** | **pstn** | **trunk-group** {**all** | *trunk-group-label*} | **voice-port** {**all** | *voice-port-label*}} [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

all	All signaling statistics.
gateway	Gateway-wide level statistics.
ip	VoIP-interface-level statistics.
pstn	PSTN-level statistics.
trunk-group	Trunk-group-level statistics. Keywords and arguments are as follows. • **all**—Statistics for all trunk groups. • *trunk-group-label*—Statistics for a specific trunk group.
voice-port	Voice-port-level statistics. Keywords and arguments are as follows: • **all**—Statistics for all voice ports. • *voice-port-label*—Statistics for a specific voice port.
mode	(Optional) Statistics in a specified mode. Keywords are as follows: • **concise**—Output contains total calls, answered calls, and answered call duration. • **verbose**—All fields contained in call statistic records (CSRs). This is the default.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. Keywords are as follows: • **all**—Pushes statistics to both the FTP and syslog servers. • **ftp**—Pushes statistics to the FTP server. • **syslog**—Pushes statistics to the syslog server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command applies only if the **voice statistics time-range** command is configured to the **since-reset** value. Voice statistics collection on the gateway is reset using the **clear voice statistics csr** command.

If you enter the **show voice statistics csr since-reset aggregation-level** command but the gateway has been configured for periodic collection or to a specific interval, the gateway will display an error message.

Examples

The following sample output shows signaling statistics for all aggregation levels since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level all

Client Type: VCSR
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-04-25T01:50:01Z

record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
,out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The following sample output shows signaling statistics for the IP aggregation level since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level ip

Client Type: VCSR
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-05-02T21:21:27Z

record_type=ip,trunk_group_id=10,voice_port_id=2,in_call=15,in_ans=15,in_fail=0,out_call=0
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The following sample output shows signaling statistics for the PSTN aggregation level since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level pstn

Client Type: VCSR
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-05-02T21:21:42Z

record_type=pstn,trunk_group_id=25,voice_port_id=2,in_call=100,in_ans=10,in_fail=90,
out_call=0,out_ans=0,out_fail=0,in_szre_d=100,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

Table 213 lists and describes the significant output fields.

Table 213 show voice statistics csr since-reset aggregation-level Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than “normal”.
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than “normal”.
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).

Table 213 show voice statistics csr since-reset aggregation-level Field Descriptions (continued)

Field	Description
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in "IP" records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
clear voice statistics csr	Clears voice-statistic collection settings on the gateway.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.

Command	Description
show voice statistics interval-tag	Displays voice statistics within a specified interval.
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies the time range to collect CSRs.

show voice statistics csr since-reset all

To display all voice call statistical information since a reset occurred, use the **show voice statistics csr since-reset all** command in privileged EXEC mode.

show voice statistics csr since-reset all [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

mode	(Optional) Statistics are displayed in a specified mode. The keywords are as follows: • **concise**—Displays output that contains total calls, answered calls, and answered call duration. • **verbose**—Displays all fields contained in call statistic records (CSRs). This is the default setting.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • **all**—Pushes statistics to both the FTP and syslog servers. • **ftp**—Pushes statistics to the FTP server. • **syslog**—Pushes statistics to the syslog server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command can also be used to display and push VoIP internal error codes (IECs).

Examples

The following example shows all of the statistics that were collected since the last reset:

```
Router# show voice statistics csr since-reset all

Client Type: VCSR
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:26Z

record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
```

```
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0

Client Type: Voice ACCT Stats
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:29Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=0,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=0
```

Table 214 lists and describes the significant output fields.

Table 214 show voice statistics csr since-reset all Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.

Table 214 show voice statistics csr since-reset all Field Descriptions (continued)

Field	Description
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than “normal”.
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than “normal”.
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than the configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.

Table 214 show voice statistics csr since-reset all Field Descriptions (continued)

Field	Description
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics interval-tag	Displays voice statistics within a specified interval.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics iec

To display Internal Error Code (IEC) statistics, use the **show voice statistics iec** command in user EXEC or privileged EXEC mode.

show voice statistics iec {**interval** *number* | **since-reboot** | **since-reset**} [**push** [**all** | **ftp** | **syslog**]]

Syntax Description

interval	Displays statistics for the specified interval.
number	The interval tag number. The range is from 1 to 36655.
since-reboot	Displays IEC statistics since the last reboot.
since-reset	Displays IEC statistics since the last reset.
push	Specifies the off-load pushing interface.
all	Indicates that IEC statistics will be off-loaded to all push interfaces.
ftp	Indicates that IEC statistics will be off-loaded to the FTP server.
syslog	Indicates that IEC statistics will be off-loaded to the syslog server.

Command Modes

User EXEC (#)
Privileged EXEC(#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **push all**, **ftp** and **syslog** keywords were added.

Usage Guidelines

Before you can display IEC statistics for a specific interval, use the **show voice statistics interval-tag** command to display available interval options. Before you display view IEC statistics since reboot, you must configure the **voice statistics type iec** command. Before you can display IEC statistics since the last reset, you must configure the **voice statistics type iec** command and the **voice statistics time-range since-reset** command.

Examples

The following is sample output from the **show voice statistics iec since-reset** command, which displays statistics since the last instance when IEC counters were cleared:

```
Router# show voice statistics iec since-reset

Internal Error Code counters
----------------------------
Counters since last reset (2002-11-28T01:55:31Z):
  SUBSYSTEM CCAPI [subsystem code 1]
      [errcode   6] No DSP resource                              5

  SUBSYSTEM SSAPP [subsystem code 4]
      [errcode   5] No dial peer match                           2
      [errcode   3] CPU high                                    96
```

```
SUBSYSTEM H323 [subsystem code 5]
    [errcode  22] No Usr Responding, H225 timeout            1
    [errcode 27] H225 invalid msg                            1
    [errcode 79] H225 chn, sock fail                        27

SUBSYSTEM VTSP [subsystem code 9]
    [errcode   6] No DSP resource                           83
```

Table 215 describes the significant fields shown in the display.

Table 215 show voice statistics iec Field Descriptions

Field	Description
SUBSYSTEM	Indicates the specific subsystem within the physical entity where the IEC was generated.
errcode	Identifies the error code within the subsystem.

The following is sample output from the **show voice statistics iec since-reset push all** command, which displays statistics since the last instance when IEC counters were cleared and off-loaded to all push interfaces.

```
Router# show voice statistics iec since-reset push all

Internal Error Code counters
----------------------------
Counters since last reset (2009-07-16T01:40:59Z):
No errors.


Router#
*Jul 16 01:43:39.530: %VSTATS-6-IEC: SEQ=1:
stats_type,version,entity_id,start_time,end_time,record_count
IEC,1,7206-2,2009-07-16T01:40:59Z,2009-07-16T01:43:39Z,0
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics	Displays voice statistics.
show voice statistics interval-tag	Displays interval options available for IEC statistics.
voice statistics time-range since-reset	Enables collection of call statistics accumulated since the last resetting of IEC counters.
voice statistics type iec	Enables collection of IEC statistics.

show voice statistics interval-tag

To display the interval numbers assigned by the gateway, use the **show voice statistics interval-tag** command in privileged EXEC mode.

show voice statistics interval-tag

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This is used to obtain the interval tag number required for the **show voice statistics csr interval accounting** and **show voice statistics csr interval aggregation** commands.

Examples

The following example shows the start and end times for specific interval tags:

```
Router# show voice statistics interval-tag

Current System Time is: 2002-4-1T010:10:00Z

    Interval-Tag   Intervals Start Time      End Time
    101            2002-3-31T010:00:00Z      2002-3-31T010:55:00Z
    105            2002-3-31T012:15:00Z      2002-3-31T012:30:00Z
```

Table 216 lists and describes the significant output fields.

Table 216 show voice statistics interval-tag Field Descriptions

Field	Description
Current System Time	Current system time of the gateway.
Interval-Tag	Interval number.
Intervals Start Time	Interval start time.
End Time	Interval end time.

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.

Command	Description
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics memory-usage

To display the memory used for collecting call statistics and to estimate the future use of memory, use the **show voice statistics memory-usage** command in privileged EXEC mode.

show voice statistics memory-usage {**all** | **csr** | **iec**}

Syntax Description

all	Memory used to collect both signaling and accounting call statistics records (CSRs).
csr	Memory used to collect signaling CSRs only.
iec	Memory used to collect Cisco internal error codes (IECs) only.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows all of the memory used at a fixed interval and since the last reset for signaling and accounting; it also shows the estimated future memory to be used.

```
Router# show voice statistics memory-usage all

*** Voice Call Statistics Record Memory Usage ***
        Fixed Interval Option -
                CSR size: 136 bytes
                Number of CSR per interval: 9
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 0
        Since Reset Option -
                CSR size: 136 bytes
                Total count of CSR: 9
                Used memory size (proximate): 1224

*** Voice Call Statistics Accounting Record Memory Usage ***
        Fixed Interval Option -
                ACCT REC size: 80 bytes
                Number of ACCT REC per interval: 1
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 0

        Since Reset Option -
                ACCT REC size: 80 bytes
                Total count of ACCT REC: 1
                Used memory size (proximate): 80
```

Table 217 lists and describes the significant output fields.

Table 217 show voice statistics memory-usage Field Descriptions

Field	Description
Voice Call Statistics Record Memory Usage	
Fixed Interval Option:	Statistics gathered for a fixed interval.
CSR size	Size of the CSR for the fixed interval.
Number of CSR per interval	Number of CSRs collected for the fixed interval.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Estimated future claimed memory size (proximate)	Amount of remaining memory available to store statistics.
Since Reset Option:	Statistics gathered since the last reset or reboot of the gateway.
CSR size	Size of the CSR since the last reset.
Total count of CSR	Total number of CSRs gathered since the last reset.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Voice Call Statistics Accounting Record Memory Usage	
Fixed Interval Option:	Statistics gathered for a fixed interval.
ACCT REC size	Accounting record size.
Number of ACCT REC per interval	Number of accounting records per interval.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Estimated future claimed memory size (proximate)	Amount of remaining memory available to store statistics.
Since Reset Option:	Statistics gathered since the last reset or reboot of the gateway.
ACCT REC size	Accounting record size.
Total count of ACCT REC	Total number of accounting records since the last reset or reboot of the gateway.
Used memory size (proximate)	Amount of memory currently being used to store statistics.

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.

Command	Description
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.

show voice trace

To display the call trace information about a specified port, use the **show voice trace** command in privileged EXEC mode.

show voice trace *interface-slot* [**detail**]

Syntax Description

interface-slot	Voice interface slot.
detail	(Optional) Displays detailed statistics of the specified port.

Command Default Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines Use the **show voice trace** command to display the call trace information about specified port. The field descriptions are self-explanatory.

Examples The following is sample output from the **show voice trace** command:

```
Router# show voice trace 1/1/1 detail
1/1/1 Stack 0:
State Transitions: timestamp (state, event) -> (state, event) ...
96.732 (S_OPEN_PEND, E_DSP_INTERFACE_INFO) ->
96.732 (S_DOWN, E_HTSP_IF_INSERVICE) ->
97.092 (S_OPEN_PEND, E_HTSP_GO_UP) ->
Event Counts (zeros not shown): (event, count)
(E_HTSP_IF_INSERVICE, 1) :(E_HTSP_GO_UP, 1) :(E_DSP_INTERFACE_INFO, 1) :
State Counts (zeros not shown): (state, count)
(S_OPEN_PEND, 2) :(S_DOWN, 1) :
Stack 1:
State Transitions: timestamp (state, event) -> (state, event) ...
97.092 (DID_NULL, E_DSP_SIG_0100) ->
97.092 (DID_INIT, E_HTSP_INSERVE) ->
97.092 (DID_PENDING, E_DSP_SIG_0100) ->
Event Counts (zeros not shown): (event, count)
(E_HTSP_INIT, 1) :(E_HTSP_INSERVE, 1) :(E_DSP_SIG_0100, 2) :
State Counts (zeros not shown): (state, count)
(DID_NULL, 2) :(DID_INIT, 1) :(DID_PENDING, 1) :
```

show voice translation-profile

To display one or more translation profiles, use the **show voice translation-profile** command in privileged EXEC mode.

show voice translation-profile [*name* | **sort** [**ascending** | **descending**]]

Syntax Description

name	Name of the translation profile to display.
sort [**ascending** | **descending**]	Display order of the translation profiles by *name*.

Command Default Ascending order

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples The following sample output displays all the voice translation profiles in ascending order:

```
Router# show voice translation-profile sort ascending

Translation Profile: 1
    Rule for Calling number:
    Rule for Called number: 1
    Rule for Redirect number:

Translation Profile: 2
    Rule for Calling number:1
    Rule for Called number: 2
    Rule for Redirect number:

Translation Profile: 6
    Rule for Calling number:1
    Rule for Called number: 6
    Rule for Redirect number:2
```

Table 217 describes the fields shown in this output.

Table 217 show voice translation-profile Field Descriptions

Field	Description
Translation Profile	Name of the translation profile.
Rule for Called number	Number of the rule used for translating called numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.

Table 217 show voice translation-profile Field Descriptions (continued)

Field	Description
Rule for Calling number	Number of the rule used for translating calling numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.
Rule for Redirect number	Number of the rule used for translating redirect numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.

Related Commands

Command	Description
voice translation-profile	Initiates a voice translation-profile definition.
voice translation-rule	Initiates a voice translation-rule definition.

show voice translation-rule

To display one or more translation rules, use the **show voice translation-rule** command in privileged EXEC mode.

show voice translation-rule [*number* | **sort** [**ascending** | **descending**]]

Syntax Description

number	Number of the translation rule to display. Valid values are from 1 to 2147483647.
sort [**ascending** | **descending**]	Display order of the translation rules by *number*.

Command Default Ascending order

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Under each translation rule are numbered subrules.

Examples The following sample output displays the translation rule number 6:

```
Router# show voice translation-rule 6

Translation-rule tag: 6
   Rule 1:
   Match pattern: 65088801..
   Replace pattern: 6508880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
```

The following sample output displays all the translation rules in ascending order:

```
Router# show voice translation-rule sort ascending

Translation-rule tag: 1
   Rule 3:
   Match pattern: 5108880...
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none

   Rule 4:
   Match pattern: 510890....
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
```

```
Translation-rule tag: 2
   Rule 1:
   Match pattern: 51088802..
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none

   Rule 2:
   Match pattern: 51088803..
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none

   Rule 3:
   Match pattern: 510889....
   Replace pattern: 5108880101
   Match type: noneReplace type: none
   Match plan: none Replace plan: none

   Rule 4:
   Match pattern: 510890....
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
```

Table 218 describes the fields shown in this output.

Table 218 show voice translation-rule Field Descriptions

Field	Description
Translation-rule tag	Number of the translation rule.
Rule	Number of the rule defined within the translation rule.
Match pattern	SED-like expression used to match incoming call information.
Replace pattern	SED-like expression used to replace *match-pattern* in the call information.
Match type	Type of incoming calls to match.
Replace type	Type to replace Match type.
Match plan	Plan of incoming calls to match.
Replace plan	Plan to replace Match plan.

Related Commands

Command	Description
rule (voice translation-rule)	Defines the SED expressions for translating calls.
test voice translation-rule	Tests the rules in a translation-rule definition.
voice translation-rule	Initiates a voice translation-rule definition.
voice translation-profile	Initiates a voice translation-profile definition.

show voice trunk-conditioning signaling

To display the status of trunk-conditioning signaling and timing parameters for a voice port, use the **show voice trunk-conditioning signaling** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning signaling [**summary** | *voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice-port	(Optional) Displays a detailed report for a specified voice port.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 as the **show voice permanent-call** command.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was renamed **show voice trunk-conditioning signaling**.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

This command displays the trunk signaling status for analog and digital voice ports on the Cisco 2600 series and the Cisco 3600 series routers.

Examples

The following is sample output from the **show voice trunk-conditioning signaling summary** command:

```
Router# show voice trunk-conditioning signaling summary

2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8  is shutdown
3/0:1 1  is shutdown
3/0:2 2  is shutdown
3/0:3 3  is shutdown
3/0:5 5  is shutdown
3/0:6(6) :
 status :
3/0:7 7  is shutdown
3/1:0 8  is shutdown
3/1:1 1  is shutdown
3/1:3 3  is shutdown
3/1:5 5  is shutdown
3/1:7 7  is shutdown
```

The following is sample output from the **show voice trunk-conditioning signaling** command for voice port 3/0:6:

```
Router# show voice trunk-conditioning signaling 3/0:6

hardware-state ACTIVE signal type is NorthamericanCAS
status :
forced playout pattern = STOPPED
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0
```

Table 219 describes significant fields in these outputs.

Table 219 show voice trunk-conditioning signaling Field Descriptions

Field	Description
current timer	Time since last signaling packets were received.
forced playout pattern	Which forced playout pattern is sent to PBX: • 0 = no forced playout pattern is sent • 1 = receive IDLE playout pattern is sent • 2 = receive OOS playout pattern is sent
hardware-state	Hardware state based on received IDLE pattern: • IDLE = both sides are idle • ACTIVE = at least one side is active
signal type	Signaling type used by lower level driver: northamerica, melcas, transparent, or external.
idle timer	Time the hardware on both sides has been in idle state.
last-ABCD	Last received or transmitted signal bit pattern.
max inter-arrival time	Maximum interval between received signaling packets.
missing	Number of missed signal packets.
mode	Signaling packet generation frequency: • Fast mode = every 4 milliseconds • Slow mode = same frequency as keepalive timer
out of seq	Number of out-of-sequence signal packets.
playout depth	Number of packets in playout buffer.
prev-seq#	Sequence number of previous signaling packet.
refill count	Number of packets created to maintain nominal length of playout packet buffer.
rx_ais_duration	Time since receipt of AIS indicator.
seq#	Sequence number of signaling packet.
sig pkt cnt	Number of transmitted or received signaling packets.
signal path	Status of signaling path.
signaling playout history	Signaling bits received in last 60 milliseconds.

Table 219 show voice trunk-conditioning signaling Field Descriptions (continued)

Field	Description
trunk_down_timer	Time since last signaling packets were received.
tx_oos_timer	Time since PBX started sending OOS signaling pattern defined by **signal pattern oos transmit**.
very late	Number of very late signaling packets.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Shows the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for voice ports.

show voice trunk-conditioning supervisory

To display the status of trunk supervision and configuration parameters for a voice port, use the **show voice trunk-conditioning supervisory** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning supervisory [**summary** | *voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice-port	(Optional) Detailed report for a specified voice port.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.4(15)T10	The output of this command was modified to report values configured by the **signal timing idle suppress-voice** command. The values for the **suppress-voice** and **resume-voice** keywords are shown as the "idle = *seconds*" and "idle_off = *milliseconds*" fields, respectively.

Usage Guidelines

This command displays the trunk supervision and configuration status for analog and digital voice ports.

Examples

The following is sample output from the **show voice trunk-conditioning supervisory summary** command for all voice ports:

```
Router# show voice trunk-conditioning supervisory summary

2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8  is shutdown
3/0:1 1  is shutdown
3/0:2 2  is shutdown
3/0:3 3  is shutdown
3/0:5 5  is shutdown
3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/0:7(7) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:0(8) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:1(1) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:3(3) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:5(5) is shutdown
3/1:7(7) is shutdown
```

The following is sample output from the **show voice trunk-conditioning supervisory** command for voice port 3/0:6:

```
Router# show voice trunk-conditioning supervisory 3/0:6

3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on, signal : on, master
    status: trunk connected
    sequence oos : idle and oos
    pattern :rx_idle = 0x0 rx_oos = 0xF
    timing : idle = 0, restart = 0, standby = 0, timeout = 40
    supp_all = 0, supp_voice = 0, keep_alive = 5
    timer: oos_ais_timer = 0, timer = 0
```

The following shows a sample trunk conditioning setting for the **voice class permanent** command and sample output from the **show voice trunk-conditioning supervisory** command that shows the values for the timeout timing field:

```
!
voice class permanent 1
  signal pattern idle transmit 0101
  signal pattern idle receive 0101
  signal pattern oos transmit 1111
  signal pattern oos receive 0101
  signal timing idle suppress-voice 10 resume-voice 150
!

Router# show voice trunk-conditioning supervisory

SLOW SCAN
0/0/0:0(1) : state : TRUNK_SC_CONNECT, voice : off , signal : on ,slave
 status: rcv IDLE, trunk connected
 sequence oos : idle and oos
 pattern :rx_idle = 0101 rx_oos = 0101 tx_idle = 0101 tx_oos =  1111
 timeout timing : idle = 10, idle_off = 150, restart = 0, standby = 0, timeout = 30
 supp_all = 0, supp_voice = 0, keep_alive = 5
 timer: oos_ais_timer = 0, timer = 0
```

Table 220 describes the significant fields shown in the display.

Table 220 show voice trunk-conditioning supervisory Field Descriptions

Field	Description
idle	Timer setting (in seconds) configured by the **suppress-voice** option of the **signal timing idle suppress-voice** command.
idle_off	Timer setting (in milliseconds) configured by the **resume-voice** option of the **signal timing idle suppress-voice** command.
keep_alive	Signaling packets periodically sent to the far end, even if there is no signal change. These signaling packets function as keep alive messages.
master	Voice port configured as "connect trunk *xxxx*."
oos_ais_timer	Time since the signaling packet with alarm indication signal (AIS) indicator was received.
pattern	4-bit signaling pattern.
restart	Restart timeout after far end is out-of-service (OOS).
rx-idle	Signaling bit pattern indicating that the far end is idle.
rx-oos	Signaling bit pattern sent to the PBX indicating that the network is OOS.

Table 220 show voice trunk-conditioning supervisory Field Descriptions (continued)

Field	Description
standby	Time before the slave side goes back to standby after the far end goes OOS.
supp_all	Timeout before suppressing transmission of voice and signaling packets to the far end after detection of PBX OOS.
supp_voice	Timeout before suppressing transmission of voice packet to the far end after detection of PBX OOS.
timeout	Timeout for nonreceipt of keepalive packets before the far end is considered to be OOS.
timeout timing	Delay between the detection of incoming seizure and when the digital signal processor (DSP)-to-Cisco IOS interaction to open up the audio path is initiated.
TRUNK_SC_CONNECT	Trunk conditioning supervisory component status.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning signaling	Displays the status of trunk-conditioning signaling and timing parameters for a voice port.
voice-class permanent	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a voice port.

show voice vtsp

To display information about the voice port configuration and Voice Telephony Service Provider (VTSP), use the **show voice vtsp** command in privileged EXEC mode.

show voice vtsp{**call** [**dspstats** | **fsm** | **log** [*call-ID*] | **verbose**] | **fork dsp-status**} [*call ID*]

Syntax Description

call	Displays the call control block information.
dspstats	(Optional) Displays the selective statistics of digital signal processor (DSP) voice channels.
fsm	(Optional) Displays information about the Finite State Machine Dump (FSM).
log *call-ID*	(Optional) Displays the call related logs. If a call ID is specified, this command displays the status of a specific call. The call ID value range is from 1 to 4294967295
verbose	(Optional) Displays the verbose output.
fork	Displays the media forking information.
dsp-status	Displays the status of media forking in the DSP.
call-ID	(Optional) Displays the status of the call. The value range is from 0x0 to 0xFFFFFFFF. >

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show voice vtsp** command to display information about the voice port configuration.

Examples

The following is sample output from the **show voice vtsp** command:

```
Router# show voice vtsp call dspstats 0x833
***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 1337, Tx Sig Pkts: 0, Tx Comfort Pkts: 181
Tx Dur(ms): 46840, Tx Vox Dur(ms): 26740, Tx Fax Dur(ms): 0
        ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 1347, Rx Signal Pkts: 0, Rx Comfort Pkts: 180
Rx Dur(ms): 46840, Rx Vox Dur(ms): 23300, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
        ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 80, Rx Delay Est(ms): 50
Rx Delay Lo Water Mark(ms): 50, Rx Delay Hi Water Mark(ms): 70
        ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 0, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
```

```
Buf Overflow Discard(ms): 0, Talkspurt Endpoint Detect Err: 0
        ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -68.5 from PBX/Phone, Tx -4.4 to PBX/Phone
TDM ACOM Levels(dBm0): +64.1, TDM ERL Level(dBm0): +10.0
TDM Bgd Levels(dBm0): -80.0, with activity being silence
        ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
        ***DSP VOICE GSMAMR-NB STATISTICS***
EncodingRate: 7 DecodingRate: 7
numEncodeChanges: 0 numDecodeChanges: 0
numCRCFail: 0 numFrameBadQuality: 0
numInvalidCMR: 0 numInvalidFrameType: 0
```

Related Commands

Command	Description
debug vtsp	Displays the state of the gateway and the call events.

show voip debug version

To display the current version of the Voice over IP debug structure, use the **show voip debug version** command in privileged EXEC mode.

show voip debug version

Command Default No default behavior or values

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples The following example shows output from the **show voip debug version** command:

```
Router# show voip debug version
voip debug version 1.0
```

Table 221 describes significant fields shown in the display.

Table 221 show voip debug version Field Descriptions

Field	Description
voip debug version 1.0	Shows the version of the debug structure.

Related Commands

Command	Description
show voip rtp connections	Displays RTP named event packets.

show voip htsp

To display the voip and hybrid transport switching protocol (HTSP) connections active in the router, use the **show voip htsp** command in privileged EXEC mode.

show voip htsp info [**controller**[**T1** *slot-number*]]

Syntax Description

info	Displays htsp related information.
controller	(Optional) Displays information about controllers such as DS3,T1,and E1.
T1	(Optional) Displays information about T1 controller.
slot-number	(Optional) controller slot number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the**show voip htsp command to** display the voip and hybrid transport switching protocol (HTSP) connections active in the router.

Examples

The following is sample output from the **show voip htsp** command:

```
Router# show voip htsp
NOTE: '-' means Not Applicable for that signalling type

  SLOT/                                                  TSP        TDM       TDM
 PORT/                                      TSP         BEAR     CONNECT   CROSS
 CHANNEL    HTSPINFO    VTSP_CDB      CDB          CHAN_T     DONE   CONNECT
=========  ==========  ==========  ==========  ==========  =======  =======
 02/00/01  0x677371E8  0x68905A48  0x67757AA4  0x677371E8     y        y
 02/00/02  0x67737780  0x00000000  0x00000000  0x00000000     n        n
 02/00/03  0x67737D18  0x68906548  0x67757584  0x67737D18     y        y
 02/00/04  0x677382B0  0x68904C88  0x677572F4  0x677382B0     y        y
 02/00/05  0x67738848  0x00000000  0x00000000  0x00000000     n        n
 02/00/06  0x67738DE0  0x00000000  0x00000000  0x00000000     n        n
 02/00/07  0x67739378  0x689054C8  0x67756B44  0x67739378     y        y
 02/00/08  0x67739910  0x68907888  0x677568B4  0x67739910     y        y
 02/00/09  0x67739EA8  0x00000000  0x00000000  0x00000000     n        n
 02/00/10  0x6773A440  0x00000000  0x00000000  0x00000000     n        n
 02/00/11  0x6773A9D8  0x68906D88  0x67756104  0x6773A9D8     y        y
 02/00/12  0x6773AF70  0x68908388  0x67755E74  0x6773AF70     y        y
 02/00/13  0x6773B508  0x00000000  0x00000000  0x00000000     n        n
 02/00/14  0x6773BAA0  0x00000000  0x00000000  0x00000000     n        n
 02/00/15  0x6773C038  0x689096C8  0x677556C4  0x6773C038     y        y
 02/00/17  0x6773C5D0  0x68909148  0x67755434  0x6773C5D0     y        y
 02/00/18  0x6773CB68  0x00000000  0x00000000  0x00000000     n        n
 02/00/19  0x6773D100  0x00000000  0x00000000  0x00000000     n        n
```

```
02/00/20  0x6773D698  0x68905788  0x67754C84  0x6773D698     y        y
02/00/21  0x6773DC30  0x68905D08  0x677549F4  0x6773DC30     y        y
02/00/22  0x6773E1C8  0x00000000  0x00000000  0x00000000     n        n
02/00/23  0x6773E760  0x00000000  0x00000000  0x00000000     n        n
02/00/24  0x6773ECF8  0x68906AC8  0x67754244  0x6773ECF8     y        y
02/00/25  0x6773F290  0x68907308  0x67753FB4  0x6773F290     y        y
02/00/26  0x6773F828  0x00000000  0x00000000  0x00000000     n        n
02/00/27  0x6773FDC0  0x00000000  0x00000000  0x00000000     n        n
02/00/28  0x67740358  0x689080C8  0x67753804  0x67740358     y        y
02/00/29  0x677408F0  0x68908908  0x67753574  0x677408F0     y        y
02/00/30  0x67740E88  0x00000000  0x00000000  0x00000000     n        n
02/00/31  0x67741420  0x68909408  0x67753054  0x67741420     y        y
02/02/01  0x67B88824  0x00000000  0x00000000      -         -        n
02/02/02  0x67B88DBC  0x00000000  0x00000000      -         -        n
02/02/03  0x67B89354  0x00000000  0x00000000      -         -        n
02/02/04  0x67B898EC  0x00000000  0x00000000      -         -        n
02/02/05  0x67B89E84  0x00000000  0x00000000      -         -        n
02/02/06  0x67B8A41C  0x00000000  0x00000000      -         -        n
02/02/07  0x67B8A9B4  0x00000000  0x00000000      -         -        n
02/02/08  0x67B8AF4C  0x00000000  0x00000000      -         -        n
02/02/09  0x67B8B4E4  0x00000000  0x00000000      -         -        n
```

Related Commands

Command	Description
debug voip vtsp	Displays information about the voice telephony service provider (VTSP).

show voip rtp connections

To display Real-Time Transport Protocol (RTP) named event packets, use the **show voip rtp connections** command in privileged EXEC mode.

show voip rtp connections [**detail**]

Syntax Description

detail	(Optional) Displays the called-party and calling-party numbers associated with a call.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.3(7)T	The **detail** keyword was added.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4(22)T	Command output was updated to show IPv6 information.

Usage Guidelines

This command displays information about RTP named event packets, such as caller ID number, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp connections** command to get caller ID, remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

The **detail** keyword allows you to identify the phone or phones that have connected two RTP call legs to create VoIP-to-VoIP or VoIP-to-POTS hairpins. If the **detail** keyword is omitted, the output does not display calls that are connected by hairpin call routing.

Examples

Table 222 describes the significant fields shown in the examples. Each line of output under "VoIP RTP active connections" shows information for one call leg. A phone call normally consists of two call legs, one connected to the calling party and one connected to the called party. The router joins (or bridges) the two call legs to make a call. The **show voip rtp connections** command shows the RTP information for H.323 and Session Initiation Protocol (SIP) calls only; it does not directly show the POTS call legs. The information for the IP phone can be seen using the **show ephone offhook** command.

The following sample output shows an incoming H.323 call that is being directed to an IP phone attached to a Cisco CallManager Express (CME) system.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
```

```
Found 1 active RTP connections
```

The following sample output shows the same call as in the previous example, but using the **detail** keyword with the command. The sample output shows the called number (1509) and calling number (8108) on both call legs (21 and 22); the called and calling numbers are the same on both legs for a simple A-to-B call. Leg 21 is the H.323 segment of the and leg 22 is the POTS segment that goes to the IP phone.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 22:called=1509 calling=8108 redirect=
   1 context 64FB3358 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following example shows the call from the previous example being transferred by extension 1509 to extension 1514. Notice that the dstCallId changed from 22 to 24, but the original call leg (21) for the transferred party is still present. This implies that H.450.2 capability was disabled for this particular call, because if H.450.2 was being used for the transfer, the transfer would have caused the incoming H.323 call leg to be replaced with a new call.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
Found 1 active RTP connections
```

The following example shows the detailed output for the same transfer as shown in the previous example. The original incoming call leg is still present (21) and still has the original called and calling numbers. The transferred call leg (24) shows 1509 (the transferring party) as the calling party and 1514 (the transfer destination) as the called party.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 24:called=1514 calling=1509 redirect=
   1 context 6466E810 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following sample output shows a cross-linked call with two H.323 call legs. The first line of output shows that the CallID for the first call leg is 7 and that this call leg is associated with another call leg that has a destination CallId of 8. The next line shows that the CallID for the leg is 8 and that it is associated with another call leg that has a destination CallId of 7. This cross-linkage between CallIds 7 and 8 shows that the first call leg is related to the second call leg (and vice versa). From this you can infer that the two call legs are actually part of the same phone call.

In an active system you can expect many lines of output that you would have to sort through to see which ones have this cross-linkage relationship. The lines showing two related call legs are not necessarily listed in adjacent order.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId   dstCallId          LocalRTP     RmtRTP         LocalIP        RemoteIP
1        7           8             16586      22346      172.27.82.2      172.29.82.2
2        8           7             17010      16590      172.27.82.2      192.168.1.29
```

```
Found 2 active RTP connections
```

The following example shows RTP information with IPv6 local and remote addresses:

```
Router# show voip rtp connections

VoIP RTP active connections :
No.  CallId   dstCallId  LocalRTP  RmtRTP   LocalIP                              RemoteIP
1     11      9          17424     18282    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6
2     12      10         18282     17424    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6

Found 2 active RTP connections
```

Table 222 show voip rtp connections Field Descriptions

Field	Description
No.	Identifier of an RTP connection in this output.
CallId	Internal call identifier of a telephony call leg (RTP connection).
dstCallId	Internal call identifier of a VoIP call leg.
LocalRTP	RTP port of the media stream for the local entity.
RmtRTP	RTP port of the media stream for the remote entity.
LocalIP	IPv4 or IPv6 address of the media stream for the local entity.
RemoteIP	IPv4 or IPv6 address of the media stream for the remote entity.
dir	0 indicates an outgoing call. 1 indicates an incoming call.
called	Extension that received the call.
calling	Extension that made the call.
redirect	Original called number if the incoming call was forwarded.
context	Internal memory address for the control block associated with the call.
xmitFunc	Internal memory address for the transmit function to which incoming RTP packets (on the H.323 and SIP side) are sent; the address for the function that delivers the packets to the ephone.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.
show ephone offhook	Displays information and packet counts for phones that are currently off hook.

show voip rtp forking

To display the Real-Time Transport Protocol (RTP) media-forking connections, use the **show voip rtp forking** command in privileged EXEC mode.

show voip rtp forking

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **show voip rtp forking** command displays information about RTP named event packets, such as type of stream, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the media-forking connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp forking** command to display the remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

Examples

The following is sample output from the **show voip rtp forking** command:

```
Router# show voip rtp forking

VoIP RTP active forks :
 Fork 1
   stream type voice-only (0): count 1
     remote ip 9.13.36.101,  remote port 20590,  local port 17596
       codec g711alaw,  logical ssrc 0x60
       packets sent 237,  packets received 413
   stream type voice+dtmf (1): count 0
   stream type dtmf-only (2): count 0
   stream type voice-nearend (3): count 1
     remote ip 9.13.36.102,  remote port 18226,  local port 17434
       codec g729r8,  logical ssrc 0x103
       packets sent 39,  packets received 0
   stream type voice+dtmf-nearend (4): count 0
   stream type voice-farend (5): count 1
     remote ip 9.13.36.120,  remote port 16912,  local port 21098
       codec g729r8,  logical ssrc 0x105
       packets sent 39,  packets received 0
   stream type voice+dtmf-farend (6): count 0
   stream type video (7): count 0
```

Table 223 describes the significant fields shown in the display.

Table 223 show voip rtp forking Field Descriptions

Field	Description
stream type	Indicates the type of stream.
count	Number of packets in the specified type of stream.
remote ip	IPv4 or IPv6 address of the media stream for the remote entity.
remote port	RTP port of the media stream for the remote entity.
local port	RTP port of the media stream for the local entity.
codec	Codec supported on the specified channel.
logical ssrc	Indicates the logical synchronization source (SSRC) for the specified channel.
packets sent	Total number of packets sent from the channel.
packets received	Total number of packets received by the channel.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.

show vrm active_calls

To display active-only voice calls either for a specific voice feature card (VFC) or for all VFCs, use the **show vrm active_calls** command in privileged EXEC mode.

show vrm active_calls {*dial-shelf-slot-number* | **all**}

Syntax Description

dial-shelf-slot-number	Slot number of the dial shelf. Range is from 0 to 13.
all	Displays list of all active calls for VFC slots.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800.

Usage Guidelines

Use this command to display active-only voice calls either for a specific VFC or for all VFCs. Each active call occupies a block of information describing the call. This information provides basically the same information as the **show vrm vdevice** command.

Examples

The following is sample output from this command specifying a dial-shelf slot number:

```
Router# show vrm active_calls 6

slot =  6 virtual voice dev (tag) =  61 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 241
Resource (vdev_common) status = 401 means :active others
tot ingress data =  24
tot ingress control  = 1308
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 22051
tot egress control  = 1304
tot egress data drops  = 0
tot egress control drops  = 0

slot =  6 virtual voice dev (tag) =  40 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 157
Resource (vdev_common) status = 401 means :active others
```

Table 224 describes significant fields shown in this output.

Table 224 show vrm active_calls Field Descriptions

Field	Description
slot	Slot where the voice card is installed.
virtual voice dev (tag)	ID number of the virtual voice device.
channel id	ID number of the channel associated with this virtual voice device.
capability list map	Bitmaps for the codec supported on that DSP channel. Values are the following: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	Last codec loaded or used.
TDM time slot	Time-division-multiplexing time slot.
Resource (vdev_common) status	Current status of the VFC.
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.

Table 224 show vrm active_calls Field Descriptions (continued)

Field	Description
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Related Commands

Command	Description
show vrm vdevices	Displays detailed information for a specific DSP or a brief summary display for all VFCs.

show vrm vdevices

To display detailed information for a specific digital signal processor (DSP) or summary information for all voice feature cards (VFCs), use the **show vrm vdevices** command in privileged EXEC mode.

show vrm vdevices {*vfc-slot-number voice-device-number* | **alarms** [*vfc-slot-number-for-alarms*] | **summary**}

Syntax Description

vfc-slot-number	Slot number of the VFC. Range is from 0 to 11.
voice-device-number	DSP number. Range is from 1 to 96.
alarms	DSP alarm statistics for all DSPs on all slots or specified slots.
vfc-slot-number-for-alarms	(Optional) Slots for which you need alarm information. If no slots are specified, alarm information for all slots is displayed.
summary	Synopsis of voice feature card DSP mappings, capabilities, and resource states.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800.
12.2(11)T	The **alarms** keyword and *vfc-slot-number-for-alarms* argument were added.

Usage Guidelines

Use this command to display detailed information for a specific DSP or a brief summary for all VFCs. The display provides information such as the number of channels, channels per DSP, bitmap of digital signal processor modules (DSPMs), DSP alarm statistics, and version numbers. This information is useful in monitoring the current state of your VFCs.

The display for a specific DSP provides information on the codec that each channel is using, if active, or on the codec that was last used and whether the channel is not currently sending cells. It also displays the state of the resource. In most cases, if there is an active call on that channel, the resource should be marked active. If the resource is marked as reset or bad, this may be an indication of a response loss for the VFC on a reset request. If this condition persists, you might experience a problem with the communication link between the router shelf and the VFC.

Examples

The following is sample output from this command specifying dial-shelf slot number and DSP number. In this particular example, the call is active so the statistics displayed are for this active call. If no calls are currently active on the device, the statistics would be for the previous (or last active) call.

```
Router# show vrm vdevices 6 1

slot =  6 virtual voice dev (tag) =  1 channel id = 1
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 0
Resource (vdev_common) status = 401 means :active others
```

```
tot ingress data =  101
tot ingress control  = 1194
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 39722
tot egress control  = 1209
tot egress data drops  = 0
tot egress control drops  = 0

slot =  6 virtual voice dev (tag) =  1 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 1
Resource (vdev_common) status = 401 means :active others
tot ingress data =  21
tot ingress control  = 1167
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 19476
tot egress control  = 1163
tot egress data drops  = 0
tot egress control drops  = 0
```

Table 225 describes significant fields shown in this output.

Table 225 show vrm vdevices Field Descriptions

Field	Description
slot	Slot in which the voice card is installed.
virtual voice dev (tag)	ID number of the virtual voice device.
channel id	ID number of the channel that is associated with this virtual voice device.
capabilities list map	Bitmaps for the codec supported on that DSP channel. Values are as follows: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000

Table 225 show vrm vdevices Field Descriptions (continued)

Field	Description
capabilities list map (continued)	• CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000
last/current codec loaded/used	Last codec loaded or used.
TDM timeslot	Time-division-multiplexing time slot.
Resource (vdev_common) status	Current status of the VFC. Values are as follows: • FREE = 0x0000 • ACTIVE_CALL = 0x0001 • BUSYOUT_REQ = 0x0002 • BAD = 0x0004 • BACK2BACK_TEST = 0x0008 • RESET = 0x0010 • DOWNLOAD_FILE = 0x0020 • DOWNLOAD_FAIL = 0x0040 • SHUTDOWN = 0x0080 • BUSY = 0x0100 • OIR = 0x0200 • HASLOCK = 0x0400 /* vdev_pool has locked port */ • DOWNLOAD_REQ = 0x0800 • RECOVERY_REQ = 0x1000 • NEGOTIATED = 0x2000 • OOS = 0x4000
tot ingress data	Total amount of data (number of packets) sent from the public switched telephone network (PSTN) side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Table 225 show vrm vdevices Field Descriptions (continued)

Field	Description
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

The following sample output displays alarm statistics for slot 6 of the DSP.

```
Router# show vrm vdevices alarms 6

----------------------ALARM STATISTICS FOR SLOT 6 ------------------------
TAG Mod DSP Chn OperStat  AlmCnt   AlmTime     AlmCause     AlmText
-------------------------------------------------------------------------
1   1   1   1   READY CD  0        0           1
                2   READY CD  0        0           1
2   1   2   1   READY CD  0        0           1
                2   READY CD  0        0           1
3   1   3   1   READY CD  0        0           1
                2   READY CD  0        0           1
4   1   4   1   READY CD  0        0           1
                2   READY CD  0        0           1
5   1   5   1   READY CD  0        0           1
                2   READY CD  0        0           1
6   1   6   1   READY CD  0        0           1
                2   READY CD  0        0           1
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
7   2   1   1   READY CD  0        0           1
                2   READY CD  0        0           1
8   2   2   1   READY CD  0        0           1
                2   READY CD  0        0           1
9   2   3   1   READY CD  0        0           1
                2   READY CD  0        0           1
10  2   4   1   READY CD  0        0           1
!
94  16  4   1   READY CD  0        0           1
                2   READY CD  0        0           1
95  16  5   1   READY CD  0        0           1
                2   READY CD  0        0           1
96  16  6   1   READY CD  0        0           1
                2   READY CD  0        0           1
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Table 226 describes significant fields shown in this output.

Table 226 show vrm vdevices alarms Field Descriptions

Field	Description
TAG	Logical tag number.
Mod	DSP module number.
DSP	DSP number within the module.
Chn	Channel number for the DSP within the module.
OperStat	Operational status of the channel.
AlmCnt	Alarm count since bootup on that channel.
AlmTime	Time at which last alarm message was received.
AlmCause	Cause of last alarm message received.

Table 226 show vrm vdevices alarms Field Descriptions (continued)

Field	Description
AlmText	Text message corresponding to the last alarm message.
Possible Values for the Operational Status of the Channel (OperStat)	
RESET	RESET state.
DOWN	DOWN state.
READY CR	CORE READY state.
READY CD	CODEC READY state.
IDLE V	VOICE IDLE state.
IDLE FAX	FAX IDLE state.
READY V	VOICE READY state.
READY FX	FAX READY state.
READY D	DTMF READY state.
UNKNOWN	UNKNOWN state.

The following is sample output from this command specifying a summary list. In the "Voice Device Mapping" area, the "C_Ac" column indicates the number of active calls for a specific DSP. If there are any nonzero numbers under the "C_Rst" and/or "C_Bad" column, a reset request was sent, but it was lost; this could mean a faulty DSP.

```
Router# show vrm vdevices summary

*********************************************************
******summary of voice devices for all voice cards*********
*********************************************************

slot = 6 major ver = 0 minor ver = 1 core type used = 2
number of modules = 16 number of voice devices (DSPs) = 96
chans per vdevice = 2 tot chans = 192 tot active calls = 178
module presense bit map = FFFF tdm mode = 1 num_of_tdm_timeslots = 384
auto recovery is on

number of default voice file (core type images) = 2
file 0 maj ver = 0 min ver = 0 core_type = 1
trough size = 2880 slop value = 0 built-in codec bitmap = 0
loadable codec bitmap = 0 fax codec bitmap = 0

file 1 maj ver = 3 min ver = 1 core_type = 2
trough size = 2880 slop value = 1440 built-in codec bitmap = 40B
loadable codec bitmap = BFC fax codec bitmap = 7E


-------------------Voice Device Mapping------------------------
Logical Device (Tag)  Module#  DSP#  C_Ac  C_Busy  C_Rst  C_Bad
---------------------------------------------------------------
1                     1        1     2     0       0      0
2                     1        2     2     0       0      0
3                     1        3     2     0       0      0
4                     1        4     2     0       0      0
5                     1        5     2     0       0      0
6                     1        6     2     0       0      0
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
7                     2        1     2     0       0      0
```

```
8                    2       2     2     0       0       0
9                    2       3     2     0       0       0
10                   2       4     1     0       0       0
11                   2       5     2     0       0       0
12                   2       6     1     0       0       0
.
.
.
91                   16      1     2     0       0       0
92                   16      2     2     0       0       0
93                   16      3     1     0       0       0
94                   16      4     2     0       0       0
95                   16      5     2     0       0       0
96                   16      6     2     0       0       0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Total active call channels = 178
Total busied out channels = 0
Total channels in reset = 0
Total bad channels = 0
Note :Channels could be in multiple states
```

Table 227 describes significant fields shown in this output.

Table 227 show vrm vdevices summary Field Descriptions

Field	Description
slot	Slot number in which the VFC is installed.
major ver	Major version of firmware running on the VFC.
minor ver	Minor version of firmware running on the VFC.
core type used	Type of DSPware in use. Values are as follows: • 1 = UBL (boot loader) • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core • 255 = invalid
number of modules	Number of modules on the VFC. Maximum number is 16.
number of voice devices (DSP)s	Number of possible DSPs. Maximum number is 96.
chans per vdevice	Number of channels (meaning calls) that each DSP can handle.
tot chans	Total number of channels.
tot active calls	Total number of active calls on this VFC.
module presense bit map	Indicates a 16-bit bitmap, each bit representing a module.
tdm mode	Time-division-multiplex bus mode. Values are as follows: • 0 = VFC is in classic mode. • 1 = VFC is in plus mode. This field should always be 1.
num_of_tdm_timeslots	Total number of calls that can be handled by the VFC.

Table 227 show vrm vdevices summary Field Descriptions (continued)

Field	Description
auto recovery	Whether auto recovery is enabled. When autorecovery is enabled, the VRM tries to recover a DSP by resetting it if, for some reason, the DSP stops responding.
number of default voice file (core type images)	Number of DSPware files in use.
number of default voice file (maj ver)	Major version of the DSPware in use.
min ver	Minor version of the DSPware in use.
core_type	Type of DSPware in use. Values are as follows: • 1 = boot loader • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core
trough size	Indirect representation of the complexity of the DSPware in use. **Note** Effective with Cisco IOS Release 12.1(5)XM, this value is no longer displayed.
slop value	Indirect representation of the complexity of the DSPware in use. **Note** Effective with Cisco IOS Release 12.1(5)XM, this value is no longer displayed.
built-in codec bitmap	Bitmap of the codec built into the DSP firmware. Values are as follows: • CC_CAP_CODEC_G711U: 0x0001 • CC_CAP_CODEC_G711A: 0x0002 • CC_CAP_CODEC_G729IETF: 0x0004 • CC_CAP_CODEC_G729a: 0x0008 • CC_CAP_CODEC_G726r16: 0x0010 • CC_CAP_CODEC_G726r24: 0x0020 • CC_CAP_CODEC_G726r32: 0x0040 • CC_CAP_CODEC_G728: 0x0080 • CC_CAP_CODEC_G723r63: 0x0100 • CC_CAP_CODEC_G723r53: 0x0200 • CC_CAP_CODEC_GSM: 0x0400 • CC_CAP_CODEC_G729b: 0x0800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000

Table 227 show vrm vdevices summary Field Descriptions (continued)

Field	Description
built-in codec bitmap (continued)	• CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000
loadable codec bitmap	Loadable codec bitmap for the loadable codecs. Values are as follows: • CC_CAP_CODEC_G711U: 0x0001 • CC_CAP_CODEC_G711A: 0x0002 • CC_CAP_CODEC_G729IETF: 0x0004 • CC_CAP_CODEC_G729a: 0x0008 • CC_CAP_CODEC_G726r16: 0x0010 • CC_CAP_CODEC_G726r24: 0x0020 • CC_CAP_CODEC_G726r32: 0x0040 • CC_CAP_CODEC_G728: 0x0080 • CC_CAP_CODEC_G723r63: 0x0100 • CC_CAP_CODEC_G723r53: 0x0200 • CC_CAP_CODEC_GSM: 0x0400 • CC_CAP_CODEC_G729b: 0x0800 • CC_CAP_CODEC_G729: = 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000
fax codec bitmap	Fax codec bitmap. Values are as follows: • FAX_NONE = 0x1 • FAX_VOICE = 0x2 • FAX_144 = 0x80 • FAX_120 = 0x40 • FAX_96 = 0x20 • FAX_72 = 0x10 • FAX_48 = 0x08 • FAX_24 = 0x04
Logical Device (Tag)	Tag number or DSP number on the VFC.
Module#	Number identifying the module associated with a specific logical device.
DSP#	Number identifying the DSP on the VFC.

Table 227 show vrm vdevices summary Field Descriptions (continued)

Field	Description
C_Ac	Number of active calls on the identified DSP.
C_Busy	Number of busied-out channels associated with the identified DSP.
C_Rst	Number of channels in the reset state associated with the identified DSP.
C_Bad	Number of defective (“bad”) channels associated with the identified DSP.
Total active call channels	Total number of active calls.
Total busied out channels	Total number of busied-out channels.
Total channels in reset	Total number of channels in the reset state.
Total bad channels	Total number of defective channels.

Related Commands

Command	Description
show vrm active_calls	Displays active-only voice calls either for a specific VFC or for all VFCs.

show vsp

To display cumulative information about voice streaming processing (VSP) sessions, use the **show vsp** command in privileged EXEC mode.

show vsp {**all** | **debug** | **session** | **statistics**}

Syntax Description

all	Displays all available information on VSP sessions, including the information specified by the other keywords listed in this table.
debug	Displays the type of debugging information that is enabled by using the **debug vsp** command.
session	Displays cumulative statistics about active VSP sessions.
statistics	Displays statistics about active VSP sessions, including memory statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use the **clear vsp statistics** command to reset the counters to 0 for the **show vsp** command.

Examples

The following is sample output from the **show vsp debug** command:

```
Router# show vsp debug

         VSP:<1>[0x62291660](0x62291660) debug_flag=0x7FF
```

The following is sample output from the **show vsp session** command:

```
Router# show vsp session

VSP_STATS:Session Statistics -
        sessions total=0; max_active=0, current=0
        session_duration last=0; max=0, min=0 ms
        pre_stream_wait last=0; max=0, min=0 ms
        stream_duration last=0; max=0, min=0 ms
        post_stream_wait last=0; max=0, min=0 ms
        stream_size last=0; max=0, min=0 bytes
        streaming_rate last=0; max=0, min=0 bytes/sec
        total_packet_count last=0; max=0, min=0 packets
        drop_packet_count last=0; max=0, min=0 packets
        particle_packet_count last=0; max=0, min=0 packets
```

The following is sample output from the **show vsp statistics** command:

```
Router# show vsp statistics

VSP_STATS:Session Statistics -
        sessions total=0; max_active=0, current=0
        session_duration last=0; max=0, min=0 ms
        pre_stream_wait last=0; max=0, min=0 ms
        stream_duration last=0; max=0, min=0 ms
        post_stream_wait last=0; max=0, min=0 ms
        stream_size last=0; max=0, min=0 bytes
        streaming_rate last=0; max=0, min=0 bytes/sec
        total_packet_count last=0; max=0, min=0 packets
        drop_packet_count last=0; max=0, min=0 packets
        particle_packet_count last=0; max=0, min=0 packets

VSP_STATS: Format Statistics -
        au_format_count=20
        wav_format_count=3
        other_format_count=0

VSP_STATS: Codec Statistics -
        codec_g729_count=4
        codec_g726_count=10
        codec_g711_count=0
        codec_g728_count=2
        codec_g723_count=5
        codec_gsm_count=2
        codec_other_count=0

VSP_STATS: Media Statistics -
        ram_count=23
        http_count=0
        smtp_count=0
        rtsp_count=0
        other_count=0

VSP_STATS:RTP Statistics -
        ts_gap_samples max=76800, min=80 samples
        [Unexpected SSRC Change (USC)]
                usc_count last=0; total=0, max=0, min=0
        [Out of sequence packet (OOSP)]
                oosp_count last=0; total=0, max=0, min=0
        [Unexpected timestamp gap (UTG)]
                max_utg_count last=0; total=0, max=0, min=0
        [Comfort Noise (CN)]
                max_cn_count last=4; total=70, max=8, min=4
        [Unexpected payload type or size (UPTS)]
                upt_count last=0; total=0, max=0, min=0; last_type=0
                ups_count last=0; total=198, max=61, min=0; last_size=2 bytes
        [Data exceeds limit (DEL)]
                del_count last=0; total=2, max=1, min=0
        [Silence exceeds timeout (SET)]
                set_count last=0; total=0, max=0, min=0

VSP_STATS:Packet Statistics -
        [Silence patching total (SPT)]
                spt_count last=296; total=7230, max=889, min=290
        [Concealment patching total (CPT)]
                cpt_count last=0; total=34, max=18, min=0
        [Normal patching total (NPT)]
                npt_count last=171; total=4249, max=453, min=106
```

Table 228 describes the fields shown in this output.

Table 228 show vsp statistics Field Descriptions

Field	Description
Session Statistics	
sessions total; max_active, current	Total number of VSP sessions since router startup or since the **clear vsp statistics** command was used. The active value should always be 0.
session_duration last; max, min	Duration of the last (most recent) session, and of the longest and shortest sessions in msecs.
pre_stream_wait last; max, min	Msecs that elapsed before the arrival of the first packet. Values are shown for last session, and for the session with the longest and shortest waits.
stream_duration last; max, min	Msecs between first packet arrival and last packet flush. Values are shown for last session, and for the session with the longest and shortest durations.
post_stream_wait last; max, min	Msecs between last packet flush and close of session.
stream_size last; max, min	Data streaming size.
streaming_rate last; max, min	Data streaming rate.
total_packet_count last; max, min	Total packets processed.
drop_packet_count last; max, min	Total packets dropped. The difference between the total packet count and packets dropped is the number of packets that have been accepted.
particle_packet_count last; max, min	Total particle packets processed.
Format Statistics	
au_format_count	Number of VSP sessions that used audio files in .au format.
wav_format_count	Number of VSP sessions that used audio files in .wav format.
other_format_count	Number of VSP sessions that used audio files of an unknown format.
Codec Statistics	
codec_g729_count	Number of VSP sessions that used the G.729 codec.
codec_g726_count	Number of VSP sessions that used the G.726 codec.
codec_g711_count	Number of VSP sessions that used the G.711 codec.
codec_g728_count	Number of VSP sessions that used the G.728 codec.
codec_g723_count	Number of VSP sessions that used the G.723 codec.
codec_gsm_count	Number of VSP sessions that used the GSM codec.
codec_other_count	Number of VSP sessions that used an unknown codec.
Media Statistics	
ram_count	Total number of RAM recordings and playouts.
http_count	Total number of HTTP recordings and playouts.
smtp_count	Total number of SMTP recordings.

Table 228 show vsp statistics Field Descriptions (continued)

Field	Description
rtsp_count	Total number of RTSP recordings and playouts.
other_count	Should always be 0.
RTP Statistics	
ts_gap_samples max min	Permissible timestamp gap in samples.
[Unexpected SSRC Change (USC)]	
usc_count last; total, max, min	Number of times that the source of the streaming has changed.
[Out of sequence packet (OOSP)]	
oosp_count last; total, max, min	Number of out-of-sequence packets.
[Unexpected timestamp gap (UTG)]	
max_utg_count last; total, max, min	Number of packets with an unexpected timestamp gap.
[Unexpected payload type or size (UPTS)]	
upt_count last; total, max, min; last_type	Number of comfort noise packets.
ups_count last; total, max, min; last_size	Number of packets with unexpected nonvoice payload sizes.
[Data exceeds limit (DEL)]	
del_count last; total, max, min	Number of times that the total recording size is larger than the preset recording size.
[Silence exceeds timeout (SET)]	
set_count last; total, max, min	Number of times that the timestamp gap is larger than the preset timeout value.
Packet Statistics	
[Silence patching total (SPT)]	
spt_count last; total, max, min	Number of silence packets that have been inserted during recording.
[Concealment patching total (CPT)]	
cpt_count last; total, max, min	Number of concealment packets that have been inserted during recording.
[Normal patching total (NPT)]	
npt_count last; total, max, min	Number of normal packets that have been patched during recording.

Related Commands

Command	Description
clear vsp statistics	Clears the statistics for VSP sessions.

show xcsp port

To display the status of a router port under the control of the external control service provider (XCSP) subsystem, use the **show xcsp port** command in privileged EXEC mode.

show xcsp port *slot-num port-num*

Syntax Description

slot-num	Slot number of the interface card. Values are as follows: • Cisco AS5350: From 0 to 3. • Cisco AS5400: From 0 to 7. • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).
port-num	Port number of the interface card. Values are as follows: • Cisco AS5350: For T1/E1, from 0 to 7. For T3, from 1 to 28. • Cisco AS5400: For T1/E1, from 0 to 7. For T3, from 1 to 28. • Cisco AS5850: For T1/E1, from 0 to 23. For T3, from 1 to 28.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	The command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5850.

Examples

The following is sample output from this command:

```
Router# show xcsp port 1 0

Slot 1 configured
Number of ports configured=1 slot state= Up
================================================
Port 0 State= Up type = 5850 24 port T1
Channel states
  0  Idle
  1  Idle
  2  Idle
  3  Idle
  4  Idle
  .
  .
  .
  22  Idle
  23  Idle
```

Table 229 describes significant fields in this output.

Note To get the field description output, you must enter the *slot-num* and *port-num* arguments for the **show xcsp port** command.

Table 229 show xcsp port Field Descriptions

Field	Descriptions
Port	Port number. Range is from 1 to 28.
State	Port state; can be Up or Down.
type	T1 or E1 ports on the AS5400: 8. T1 or E1 ports on the AS5850: 24. T3 ports on the AS5400 and AS5850: 28.
Channel states	Channel states. Values are as follows: • Blocked • Connection in progress • Cot Check In Progress • Cot Check Pending • Down • Idle • In Release in progress • In Use • Invalid • Loopback • Not Present • Out of Service • Out Release in progress • Playing Tone • Shutdown

Related Commands

Command	Description
show xcsp slot	Displays the status of XCSP slots.

show xcsp slot

To display the status of a router slot under the control of the external control service provider (XCSP) subsystem, use the **show xcsp slot** command in privileged EXEC mode.

show xcsp slot *slot-num*

Syntax Description

slot-num	The slot number of the T1 or E1 interface card. Values are as follows: • Cisco AS5350: From 0 to 3. • Cisco AS5400: From 1 to 7. • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	The command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5850.

Examples

The following is sample output from this command:

```
Router# show xcsp slot 1

Slot 1 configured
Number of ports configured=1 slot state= Up
```

Table 230 describes significant fields shown in this output.

Table 230 show xcsp slot Field Descriptions

Field	Description
slot state	Slot state; can be either Up or Down.

Related Commands

Command	Description
show xcsp port	Displays the status of XCSP ports.

shut

To shut down a set of digital signal processors (DSPs) on the Cisco 7200 series router, use the **shut** command in DSP configuration mode. To put DSPs back in service, use the **no** form of this command.

shut *number*

no shut *number*

Syntax Description

number	Number of DSPs to be shut down.

Command Default No shut

Command Modes DSP configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.1(1)T	This command was modified to add information about DSP groups.

Usage Guidelines This command applies to VoIP on the Cisco 7200 series routers.

Examples The following example shuts down two sets of DSPs:

```
shut 2
```

shutdown (Annex G neighbor)

To disable the service relationships requirement for border elements, use the **shutdown** command in config-nxg-neigh-srvc mode. To enable the service relationship for border elements, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The Annex G neighbor is shut down.

Command Modes

Annex G neighbor service

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **no shutdown** command verifies that a domain name has been configured and ensures that the border element has been configured to reject messages from unknown "stranger" border elements.

Examples

The following example enables the border element:

```
Router(config-nxg-neigh-srvc)# no shutdown
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time that a border element attempts delivery.

shutdown (Annex G)

To shut down the Annex G border element (BE), use the **shutdown** command in Annex G configuration mode. To reinstate the Annex G BE, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The Annex G border element is not shut down.

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

While the Annex G BE is in shutdown state, all Annex G messages received from neighbors are ignored and the colocated gatekeeper does not use the Annex G BE for address resolution.

Examples

The following example shuts the BE down:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# shutdown
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.
show call-router status	Displays the Annex G BE status.

shutdown (dial peer)

To change the administrative state of the selected dial peer from up to down, use the **shutdown** command in dial peer configuration mode. To change the administrative state of this dial peer from down to up, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default No shutdown

Command Modes Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.1(1)	This command was modified for store-and-forward fax.

Usage Guidelines When a dial peer is shut down, you cannot initiate calls to that peer.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples The following example changes the administrative state of voice telephony (plain old telephone service [POTS]) dial peer 10 to down:

```
dial-peer voice 10 pots
shutdown
```

The following example changes the administrative state of voice telephony (POTS) dial peer 10 to up:

```
dial-peer voice 10 pots
no shutdown
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the dial-peer tag number.

shutdown (DSP Farm profile)

To disable the digital signal processor (DSP) farm profile, use the **shutdown** command in DSP farm profile configuration mode. To allocate DSP farm resources and associate with the application, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes DSP farm profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines It is essential that the profile be disabled by using the **shutdown** command before a DSP farm profile is updated.

Examples The following example allocates DSP farm resources and associates with the application:

```
Router(config-dspfarm-profile)# no shutdown
```

Related Commands

Command	Description
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters the DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.

shutdown (gatekeeper)

To disable the gatekeeper, use the **shutdown** command in gatekeeper configuration mode. To enable the gatekeeper, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (shut down)

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

The gatekeeper does not have to be enabled before you can use the other gatekeeper configuration commands. In fact, it is recommended that you complete the gatekeeper configuration before bringing up the gatekeeper because some characteristics may be difficult to alter while the gatekeeper is running, as there may be active registrations or calls.

The **no shutdown** command enables the gatekeeper, but it does not make the gatekeeper operational. The two exceptions to this are as follows:

- If no local zones are configured, a **no shutdown** command places the gatekeeper in INACTIVE mode waiting for a local zone definition.
- If local zones are defined to use an HSRP virtual address, and the HSRP interface is in STANDBY mode, the gatekeeper goes into HSRP STANDBY mode. Only when the HSRP interface is ACTIVE does the gatekeeper go into the operational UP mode.

Examples

The following command disables a gatekeeper:

```
shutdown
```

Related Commands

Command	Description
shutdown (gateway)	Shuts down all VoIP call service on a gateway.

shutdown (gateway)

To shut down all VoIP call service on a gateway, use the **shutdown** command in voice service configuration mode. To enable VoIP call service, use the **no** form of this command.

shutdown [**forced**]

no shutdown

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.

Command Default

Call service is enabled

Command Modes

Voice service configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows VoIP call service being shut down on a Cisco gateway:

```
voice service voip
shutdown
```

The following example shows VoIP call service being enabled on a Cisco gateway:

```
voice service voip
no shutdown
```

Related Commands

Command	Description
shutdown (gatekeeper)	Disables the gatekeeper.

shutdown (mediacard)

To disable a selected media card, use the **shutdown** command in mediacard configuration mode. To enable a selected media card, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Media card configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines Use the **no shutdown** command at the end of media card configuration. If there are any active connections when you disable the media card, the Digital Signal Processor Resource Manager (DSPRM) displays a warning message indicating that the DSP resources allocated on other media cards for some of the resource pool in this media card will be removed or that there are active connections available in this resource pool and prompts you for a response. Profiles that use resources on this card must be brought up separately after using this command.

Examples The following example shows how to enable a media card:

```
no shutdown
```

Related Commands

Command	Description
resource-pool	Creates a DSP resource pool on the selected media card.

shutdown (auto-config application)

To disable an auto-configuration application for download, use the **shutdown** command in auto-config application configuration mode. To enable an auto-configuration application for download, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no keywords or arguments.

Command Default Disabled

Command Modes Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples The following example shows the **shutdown** command used to enable an auto-configuration application for download:

```
Router(auto-config-app)# no shutdown
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
show auto-config	Displays the current status of auto-configuration applications.

shutdown (RLM)

To shut down all of the links under the RLM group, use the **shutdown** command in RLM configuration mode. RLM does not try to reestablish those links until the command is negated. To disable this function, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
timer	Overwrites the default setting of timeout values.

shutdown (settlement)

To deactivate the settlement provider, use the **shutdown** command in settlement configuration mode. To activate a settlement provider, use the **no** version of the command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The default status of a settlement provider is deactivated. The settlement provider is down.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use this command at the end of the configuration of a settlement server to bring up the provider. This command activates the provider. Otherwise, transactions do not go through the provider to be audited and charged. Use the **shutdown** command to deactivate the provider.

Examples

The following example enables a settlement server:

```
settlement 0
 no shutdown
```

The following example disables a settlement server:

```
settlement 0
 shutdown
```

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.

Command	Description
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

shutdown (voice-port)

To take the voice ports for a specific voice interface card offline, use the **shutdown** command in voice-port configuration mode. To put the ports back in service, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

Shutdown

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

When you use this command, all ports on the voice interface card are disabled. When you use the **no** form of the command, all ports on the voice interface card become enabled. A telephone connected to an interface hears silence when a port is shut down.

Examples

The following example takes voice port 1/1/0 offline:

```
voice-port 1/1/0
shutdown
```

Related Commands

Command	Description
shutdown (port)	Disables a port.

signal

To specify the type of signaling for a voice port, use the **signal** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

Foreign Exchange Office (FXO) and Foreign Exchange Station (FXS) Voice Ports

signal {**groundstart** | **loopstart** [**live-feed**]}

no signal {**groundstart** | **loopstart**}

Ear and mouth (E&M) Voice Ports

signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}

no signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}

Centralized Automatic Message Accounting (CAMA) Ports

signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}

no signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}

Syntax Description

groundstart	Specifies the use of groundstart signaling. Used for FXO and FXS interfaces. Groundstart signaling allows both sides of a connection to place a call and to hang up. **Note** The CAMA version of this keyword is **groundstart**. Both forms operate identically.
loopstart	Specifies the use of loop start signaling. Used for FXO and FXS interfaces. With loopstart signaling, only one side of a connection can hang up. This is the default setting for FXO and FXS voice ports. **Note** The CAMA version of this keyword is **loopstart**. Both forms operate identically.
live-feed	(Optional) Enables an MOH audio stream from a live feed to be directly connected to the router through an FXO port.
delay-dial	The calling side seizes the line by going off-hook on its E-lead. After a timing interval, the calling side looks at the supervision from the called side. If the supervision is on-hook, the calling side starts sending information as dual tone multifrequency (DTMF) digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. Used for E&M tie trunk interfaces.
immediate	The calling side seizes the line by going off-hook on its E-lead and sends address information as DTMF digits. Used for E&M tie trunk interfaces.
lmr	Specifies the use of Land Mobile Radio signaling.

wink-start	The calling side seizes the line by going off-hook on its E-lead then waits for a short off-hook "wink" indication on its M-lead from the called side before sending address information as DTMF digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.
cama	Selects and configures the port for 911 calls.
kp-0-npa-nxx-xxxx-st	10-digit transmission. The E.164 number is fully transmitted.
kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st	Supports CAMA Signaling with ANI/Pseudo ANI (PANI).
kp-0-nxx-xxxx-st	7-digit automatic number identification (ANI) transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted.
kp-2-st	Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) digit in the lookup table, or when the calling number is fewer than ten digits in length. (NPA digits are not available.)
kp-npd-nxx-xxxx-st	8-digit ANI transmission, where the NPD is a single multifrequency (MF) digit that is expanded into the NPA. The NPD table is preprogrammed in the sending and receiving equipment (on each end of the MF trunk); for example: 0 = 415, 1 = 510, 2 = 650, 3 = 916 05550100 = (415) 555-0100, 15550100 = (510) 555-0100, and so on. NPD range is from 0 to 3.

Command Default

FXO and FXS interfaces: **loopstart**
E&M interfaces: **wink-start**
CAMA interfaces: **loopstart**

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(11)T	This command was modified to support ANI transmission.
12.3(4)XD	The **lmr** keyword was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(9)T	The **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st** keyword was added to support CAMA Signaling with ANI/Pseudo ANI (PANI).
12.4(11)XJ	The **live-feed** keyword was added.
12.4(15)T	The **live-feed** keyword was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command applies to analog voice ports only. A voice port must be shut down and then activated before the configured values take effect.

For an E&M voice port, this command changes only the signal value for the selected voice port.

For an FXO or FXS voice port, this command changes the signal value for both voice ports on a voice port module (VPM). If you change the signal type for an FXO voice port on Cisco 3600 series routers, you need to move the appropriate jumper in the voice interface card of the voice network module. For more information about the physical characteristics of the voice network module, see the installation documentation that came with your voice network module.

Some PBXs miss initial digits if the E&M voice port is configured for immediate start signaling. Immediate start signaling should be used for dial pulse outpulsing only and only on circuits for which the far end is configured to accept digits within a few milliseconds of seizure. Delay dial signaling, which is intended for use on trunks and not lines, relies on the far end to return an off-hook indication on its M-lead as soon as the circuit is seized. When a receiver is attached, the far end removes the off-hook indication to indicate that it is ready to receive digits. Delay dial must be configured on both ends to work properly. Some non-Cisco devices have a limited number of DTMF receivers. This type of equipment must delay the calling side until a DTMF receiver is available.

To specify which VIC-2CAMA ports are designated as dedicated CAMA ports for emergency 911 calls, use the **signal cama** command. No two service areas in the existing North American telephony infrastructure supporting E911 calls have identical service implementations, and many of the factors that drive the design of emergency call handling are matters of local policy and therefore outside the scope of this document. Local policy determines which ANI format is appropriate for the specified Physical Service Access Point (PSAP) location.

The following four types of ANI transmittal schemes are based on the actual number of digits transmitted toward the E911 tandem. In each instance, the actual calling number is proceeded with a key pulse (KP) followed by an information (I) field or a NPD, which is then followed by the ANI calling number, and finally is followed by a start pulse (ST), STP, ST2P, or ST3P, depending on the trunk group type in the PSTN and the traffic mix carried.

The information field is one or two digits, depending on how the circuit was ordered originally. For one-digit information fields, a value of 0 indicates that the calling number is available. A value of 1 indicates that the calling number is not available. A value of 2 indicates an ANI failure. For a complete list of values for two-digit information fields, see *SR-2275: Telcordia Notes on the Networks* at www.telcordia.com.

- 7-digit transmission (**kp-0-nxx-xxxx-st**):

  The calling phone number is transmitted, and the NPA is implied by the trunk group and not transmitted.

- 8-digit transmission (**KP-npd-nxx-xxxx-st**):

  The I field consists of single-digit NPD-to-NPA mapping. When the calling party number of 415-555-0122 places a 911 call, and the Cisco 2600 series or Cisco 3600 series has an NPD (0)-to-NPA (415) mapping, the NPA signaling format is received by the selective router at the central office (CO).

  Note NPD values greater than 3 are reserved for signifying error conditions.

- 10-digit transmission (**kp-0-npa-nxx-xxxx-st)**:

  The E.164 number is fully transmitted.

- 20-digit transmission (**kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st)**:

  Twenty digits support (two 10 digit numbers) on FGD-OS in the following format, KP+II+10 digit ANI+ST+KP+7/10 digit PANI+ ST

- kp–2–st transmission (**kp–2–st**):

  kp–2–st transmission is used if the PBX is unable to out-pulse the ANI. If the ANI received by the Cisco router is not as per configured values, kp–2–st is transmitted. For example, if the voice port is configured for out-pulsing a ten-digit ANI and the 911 call it receives has a seven-digit calling party number, the router transmits kp–2–st.

  Note Emergency 911 calls are not rejected for an ANI mismatch. The call establishes a voice path. The E911 network, however, does not receive the ANI.

Examples

The following example configures groundstart signaling on the Cisco 3600 series as the signaling type for a voice port, which means that both sides of a connection can place a call and hang up:

```
voice-port 1/1/1
 signal groundstart
```

The following example configures a ten-digit ANI transmission:

```
Router(config)# voice-port 1/0/0
Router(config-voiceport)# signal cama kp-0-npa-nxx-xxxx-st
```

The following example configures 20-digit CAMA Signaling with ANI/Pseudo ANI:

```
Router(config-voiceport)# signal cama KP-0-NPA-NXX-XXXX-ST-KP-YYY-YYY-YYYY-ST
```

Related Commands

Command	Description
ani mapping	Preprograms the NPA, or area code, into a single MF digit.

signal did

To enable direct inward dialing (DID) on a voice port, use the **signal did** command in voice-port configuration mode. To disable DID and reset to loop-start signaling, use the **no** form of this command.

signal did {**immediate-start** | **wink-start** | **delay-start**}

no signal did

Syntax Description

immediate-start	Enables immediate-start signaling on the DID voice port.
wink-start	Enables wink-start signaling on the DID voice port.
delay-start	Enables delay-dial signaling on the DID voice port.

Command Default No default behavior or values

Command Modes Voice-port configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Examples The following example configures a voice port with immediate-start signaling enabled:

```
Router# voice-port 1/17
Router (config-voiceport)# signal did immediate-start
```

signal keepalive

To configure the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks, use the **signal keepalive** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal keepalive {*seconds* | **disabled**}

no signal keepalive {*seconds* | **disabled**}

Syntax Description

seconds	Keepalive signaling packet interval, in seconds. Range is from 1 to 65535. Default is 5 seconds.
disabled	Specifies that no keepalive signals are sent.

Command Default

seconds: 5 seconds

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.3(7)T	The **disabled** keyword was added.

Usage Guidelines

Before configuring the keepalive signaling interval, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer using the **voice-class permanent** (dial peer) command.

To avoid sending keepalive signals to a multicasting network with no specified destination, we recommend that you use the **disabled** keyword when configuring this command for use in networks that use connection trunk connections and multicasting.

Examples

The following example shows the keepalive signaling interval set to 3 seconds for voice class 10:

```
voice class permanent 10
 signal keepalive 3
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal pattern

To define the ABCD bit patterns that identify the idle and out-of-service (OOS) states for Cisco trunks and FRF.11 trunks, use the **signal pattern** command in voice-class configuration mode. To remove the patterns from the voice class, use the **no** form of this command.

signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*

no signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*

Syntax Description

idle receive	Signaling pattern for identifying an idle message from the network. Also defines the idle signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos idle-only** or **signal sequence oos both** command is configured.
idle transmit	Signaling pattern for identifying an idle message from the PBX.
oos receive	OOS signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos oos-only** or **signal sequence oos both** command is configured.
oos transmit	Signaling pattern for identifying an OOS message from the PBX.
bit-pattern	ABCD bit pattern. Range is from 0000 to 1111.

Command Default

idle receive
Near-end E&M: 0000 (for T1) or 0001 (for E1)
Near-end FXO loop start: 0101
Near-end FXO ground start: 1111
Near-end FXS: 0101
Near-end MELCAS: 1101

idle transmit
Near-end E&M: 0000
Near-end FXO: 0101
Near-end FXS loop start: 0101
Near-end FXS ground start: 1111
Near-end MELCAS: 1101

oos receive
Near-end E&M: 1111
Near-end FXO loop start: 1111
Near-end FXO ground start: 0000
Near-end FXS loop start: 1111
Near-end FXS ground start: 0101
Near-end MELCAS: 1111

oos transmit
No default signaling pattern is defined.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	Default signaling patterns were defined.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the signaling pattern, you must use the **voice-class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you define the voice class, you assign it to a dial peer.

Idle Patterns

An idle state is generated if the router detects an idle signaling pattern coming from either direction. If an idle pattern is configured for only one direction (transmit or receive), an idle state can be detected only in the configured direction. Therefore, you should normally enter both the **idle receive** and the **idle transmit** keywords.

To suppress voice packets whenever the transmit or receive trunk is in the idle state, use the **idle receive** and **idle transmit** keywords in conjunction with the **signal timing idle suppress-voice** command.

OOS Patterns

An OOS state is generated differently in each direction under the following conditions:

- If the router detects an **oos transmit** signaling pattern sent from the PBX, the router transmits the **oos transmit** signaling pattern to the network.
- If the **signal timing oos timeout** timer expires and the router receives no signaling packets from the network (network is OOS), the router sends an **oos receive** signaling pattern to the PBX. (The **oos receive** pattern is not matched against the signaling packets received from the network; the receive packets indicate an OOS condition directly by setting the AIS alarm indication bit in the packet.)

To suppress voice packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-voice** command.

To suppress voice and signaling packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-all** command.

PBX Busyout

To "busy out" a PBX if the network connection fails, set the **oos receive** pattern to match the seized state (busy), and set the **signal timing oos** timeout value. When the timeout value expires and no signaling packets are received, the router sends the **oos receive** pattern to the PBX.

Use the busy seized pattern only if the PBX does not have a specified pattern for indicating an OOS state. If the PBX has a specific OOS pattern, use that pattern instead.

Examples

The following example, beginning in global configuration mode, configures the signaling bit pattern for the idle receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example, beginning in global configuration mode, configures the signaling bit pattern for the out-of-service receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example restores default signaling bit patterns for the receive and transmit idle states:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice
 no signal pattern idle receive
 no signal pattern idle transmit
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example configures nondefault signaling bit patterns for the receive and transmit out-of-service states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies a dial-peer type.
signal timing idle suppress-voice	Specifies the length of time before voice traffic is stopped after a trunk goes into the idle state.
signal timing oos	Configures the signal timing parameter for the OOS call state.
signal timing oos slave-standby	Specifies that a slave port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Stops sending voice and signaling packets to the network if a transmit OOS signaling pattern id detected from the PBX for a specified time.
signal timing oos suppress-voice	Stops sending voice packets to the network if a transmit OOS signaling pattern is detected from the PBX for a specified time.

Command	Description
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal sequence oos

To specify which signaling pattern is sent to the PBX when the far-end keepalive message is lost or an alarm indication signal (AIS) is received from the far end, use the **signal sequence oos** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal sequence oos {**no-action** | **idle-only** | **oos-only** | **both**}

no signal sequence oos

Syntax Description

no-action	No signaling pattern is sent.
idle-only	Only the idle signaling pattern is sent.
oos-only	Only the out-of-service (OOS) signaling pattern is sent.
both	Both idle and OOS signaling patterns are sent. This is the default value.

Command Default

Both idle and OOS signaling patterns are sent.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the idle or OOS signaling patterns to be sent, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

Use the **signal sequence oos** command to specify which signaling pattern) to send. Use the **signal pattern idle receive** or the **signal pattern oos receive** command to define the bit patterns of the signaling patterns if other than the defaults.

Examples

The following example, beginning in global configuration mode, defines voice class 10, sets the **signal sequence oos** command to send only the idle signal pattern to the PBX, and applies the voice class configuration to VoFR dial peer 100.

```
voice-class permanent 10
 signal-keepalive 3
 signal sequence oos idle-only
 signal timing idle suppress-voice
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Specifies the length of time before the router stops sending voice packets after a trunk goes into the idle state.
signal timing oos	Specifies that a permanent voice connection be torn down and restarted after the trunk has been OOS for a specified time.
signal timing oos slave-standby	Specifies that a slave port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Configures the router or concentrator to stop sending voice and signaling packets to the network if it detects an OOS signaling pattern from the PBX for a specified time.
signal timing oos suppress-voice	Configures the router or concentrator to stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX for a specified time.
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing idle suppress-voice

To configure the signal timing parameter for the idle state of a call, use the s**ignal timing idle suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]

no signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]

Syntax Description

seconds	Duration of the idle state, in seconds, before the voice traffic is stopped. Range is from 0 to 65535.
resume-voice	(Optional) Sets a timer that controls the delay between when trunk activity is detected and when active packetization of voice resumes.
milliseconds	(Optional) Duration of the delay, in milliseconds (ms), for the resume-voice timer. Range is from 40 to 5000. Default is 500 ms.

Command Default

No signal timing idle suppress-voice timer is configured.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 platform.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to simplify the configuration process.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.4(15)T10	This command was modified to add the **resume-voice** *milliseconds* option.

Usage Guidelines

Before configuring the signal timing idle suppress-voice timer, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

The **signal timing idle suppress-voice** command is used when the **signal-type** command is set to **transparent** in the dial peer for the Cisco trunk or FRF.11 trunk connection. The router stops sending voice packets when the timer expires. Signaling packets are still sent.

To detect an idle trunk state, the router or concentrator monitors both transmit and receive signaling for the idle transmit and idle receive signaling patterns. These can be configured by the **signal pattern idle transmit** or **signal pattern idle receive** command, or they can be the defaults. The default idle receive pattern is the idle pattern of the local voice port. The default idle transmit pattern is the idle pattern of the far-end voice port.

In some circumstances, the default delay of 500 ms between the detection of incoming seizure and the opening of the audio path may cause a timing issue.

If, during this delay of 500 ms, the near-end originating PBX has already received the acknowledgement from the far-end PBX to begin playing out digits and the audio path is not yet open, the first Dual Tone Multi-Frequency (DTMF) digit might be lost over the permanent trunk.

This loss of the first DTMF digit can occur if a Cisco voice gateway has the following trunk conditioning setting:

```
!
voice class permanent 1
signal pattern idle transmit 0000
signal pattern idle receive 0000
signal pattern oos transmit 1111
signal pattern oos receive 1111
signal timing idle suppress-voice 10

!
```

The **resume-voice** *milliseconds* option has been added in Release 12.4(15)T10 to modify the delay timer and reduce the wait time. We recommend that you specify a delay of less than 500 ms to avoid the loss of any digits due to the possible discrepancy between the detection of incoming seizure and the opening of the audio path.

The output of the **show voice trunk-conditioning supervisory** command has been modified in Release 12.4(15)T10 to report values for the **suppress-voice** and **resume-voice** keywords (of the **signal timing idle suppress-voice** command) as the "idle = *seconds*" and "idle_off = *milliseconds*" fields, respectively.

Examples

The following example, beginning in global configuration mode, sets the signal timing idle suppress-voice timer to 5 seconds for the idle state on voice class 10:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 signal timing idle suppress-voice 5
 exit
 dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

The following example defines voice class 10, sets the idle detection time to 5 seconds, configures the trunk to use the default transmit and receive idle signal patterns, and applies the voice class configuration to VoFR dial peer 100:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice 5
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for a voice port.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and OOS states for Cisco trunks and FRF.11 trunks.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos

To configure the signal timing parameter for the out-of-service (OOS) state of the call, use the **signal timing oos** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos {**restart** | **slave-standby** | **suppress-all** | **suppress-voice** | **timeout**} *seconds*

no signal timing oos {**restart** | **slave-standby** | **suppress-all** | **suppress-voice** | **timeout**} *seconds*

Syntax Description

restart	If no signaling packets are received for this period, the permanent voice connection is torn down and an attempt to achieve reconnection is made.
slave-standby	If no signaling packets are received for this period, a slave port returns to its initial standby state. This option applies only to slave ports (ports configured using the **connection trunk number answer-mode** command).
suppress-all	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending all packets to the network.
suppress-voice	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending voice packets to the network. signaling packets continue to be sent with the alarm indication set (AIS).
timeout	If no signaling packets are received for this period of time, the router sends the configured receive OOS pattern to the PBX. Also, the router stops sending voice packets to the network. Use this option to perform busyout to the PBX.
seconds	Duration, in seconds, for the above settings. Range is from 0 to 65535.

Command Default

No signal timing OOS pattern parameters are configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(4)T	This command was introduced.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

You can enter several values for this command. However, the **suppress-all** and **suppress-voice** options are mutually exclusive.

Examples

The following example, beginning in global configuration mode, configures the signal timeout parameter for the OOS state on voice class 10. The **signal timing oos timeout** command is set to 60 seconds.

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of the call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos restart

To specify that a permanent voice connection be torn down and restarted after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos restart** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos restart *seconds*

no signal timing oos restart

Syntax Description

seconds	Delay duration, in seconds, for the restart attempt. Range is from 0 to 65535. There is no default.

Command Default

No restart attempt is made if the trunk becomes OOS.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. You then assign the voice class to a dial peer.

The **signal timing oos restart** command is valid only if the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos restart** command does not start until the trunk is OOS.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds and sets the **restart** time to 30 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos restart 30
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos slave-standby

To configure a slave port to return to its initial standby state after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos slave-standby** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos slave-standby *seconds*

no signal timing oos slave-standby

Syntax Description

seconds	Delay duration, in seconds. If no signaling packets are received for this period, the slave port returns to its initial standby state. Range is from 0 to 65535. There is no default.

Command Default

The slave port does not return to its standby state if the trunk becomes OOS.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

If no signaling packets are received for the specified delay period, the slave port returns to its initial standby state. The **signal timing oos slave-standby** command is valid only if both of the following conditions are true:

- The **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos slave-standby** command does not start until the trunk is OOS.
- The voice port is configured as a slave port with the **connection trunk digits answer-mode** command.

Examples

The following example, beginning in global configuration mode, creates a voice port as a slave voice port, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the return-to-slave-standby time to 120 seconds:

```
voice-port 1/0/0
 connection trunk 5559262 answer-mode
 exit
 voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos slave-standby 120
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-all

To configure the router or concentrator to stop sending voice and signaling packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-all** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-all *seconds*

no signal timing oos suppress-all

Syntax Description

seconds	Delay duration, in seconds, before packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-all** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default **oos transmit** signaling pattern.)

The **signal timing oos suppress-all** command is valid whether or not the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-all** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS timeout time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-all 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-voice

To configure the router or concentrator to stop sending voice packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-voice *seconds*

no signal timing oos suppress-voice

Syntax Description

seconds	Delay duration, in seconds, before voice-packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-voice** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default oos transmit signaling pattern.)

The **signal timing oos suppress-voice** s command is valid whether or not the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-voice** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS timeout time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-voice 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos timeout

To change the delay time between the loss of signaling packets from the network and the start time for the out-of-service (OOS) state, use the **signal timing oos timeout** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos timeout [*seconds* | **disabled**]

no signal timing oos timeout

Syntax Description

seconds	(Optional) Delay duration, in seconds, between the loss of signaling packets and the beginning of the OOS state. Range is from 1 to 65535. Default is 30.
disabled	(Optional) Deactivates the detection of packet loss. If no signaling packets are received from the network, the router does not sent an OOS pattern to the PBX and it continues sending voice packets to the network. Use this option to disable busyout to the PBX.

Command Default No signal timing OOS pattern parameters are configured.

Command Modes Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

You can use the **signal timing oos timeout** command to enable busyout to the PBX.

The **signal timing oos timeout** command controls the starting time for the **signal timing oos restart** and **signal timing oos slave-standby** commands. If this command is entered with the **disabled** keyword, the **signal timing oos restart** and **signal timing oos slave-standby** commands are ineffective.

Examples

The following example, beginning in global configuration mode, creates voice class 10 and sets the OOS timeout time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signaling forward

To enable a Cisco IOS gateway to forward the Generic Transparency Descriptor (GTD) payload to another gateway or gatekeeper system-wide, use the **signaling forward** command in global configuration mode. To disable forwarding, use the **no** form of this command.

signaling forward {**conditional | unconditional | none**}

no signaling forward

Syntax Description

conditional	Changes the forwarding behavior on the basis of the target defined in the **session target** command. If the target is a non-Registration, Admission, and Status (RAS) target, the original signaling payload is forwarded to the H.323 endpoint using H.225 messages.
unconditional	Tunnels the GTD payload in the H.225 SETUP message to the final endpoint in the network. The gatekeeper sends its own GTD back to itself in this situation.
none	Prevents the gateway from forwarding the GTD payload to endpoints in the network.

Command Default

Signaling forwarding is conditional.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5850.

Usage Guidelines

This command is used with the Cisco PGW 2200 in the Cisco SS7 Interconnect for Voice Gateways solution. You must configure the Cisco PGW 2200 to encapsulate SS7 ISUP messages in GTD format before using this command on the Cisco gateway.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISDN User Part (ISUP) GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

This command does not prevent sending the GTD to a gatekeeper. Any GTD on the originating gateway is sent to the gatekeeper for use in routing decisions. To prevent GTD creation, the **signal-end-to-end** command-line interface (CLI) option on the R2 interfaces should be disabled, and the Cisco PGW 2200 should be configured not to send GTD to the gateway.

Examples

The following example sets unconditional signal forwarding on a system-wide basis, where the GTD payload is tunneled in H.225 SETUP messages to endpoints:

```
Router(config)# voice service voip
Router(conf-voi-serv)# signaling forward unconditional
Router(conf-voi-serv)# ^Z
Router# show running-config

Building configuration...

Current configuration : 4201 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
!
.
.
.
!
voice service voip
 signaling forward unconditional
 h323
!
.
.
.
```

Related Commands

Command	Description
clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
session target	Specifies a network-specific address for a dial peer.

signaling forward (dial peer)

To enable a Cisco IOS gateway to forward the Generic Transparency Descriptor (GTD) payload to another gateway or gatekeeper for an individual dial peer, use the **signaling forward** command in dial peer configuration mode. To disable forwarding, use the **no** form of this command.

signaling forward {**conditional** | **unconditional** | **none**}

no signaling forward

Syntax Description

conditional	Changes the forwarding behavior on the basis of the target defined in the **session target** command. If the target is a non-Registration, Admission, and Status (RAS) target, the original signaling payload is forwarded to the H.323 endpoint using H.225 messages.
unconditional	Tunnels the GTD payload in the H.225 SETUP message to the final endpoint in the network. The gatekeeper sends its own GTD back to itself in this situation.
none	Prevents the gateway from passing the GTD payload to endpoints in the network.

Command Default

The default is the value that is configured system-wide, or conditional if signaling forward is not configured system-wide.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5850.

Usage Guidelines

This command is used with the Cisco PGW 2200 Signaling Controller in the Cisco SS7 Interconnect for Voice Gateways solution. You must configure the Cisco PGW 2200 to encapsulate SS7 ISUP messages in GTD format before using this command on the Cisco gateway.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISDN User Part (ISUP) GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

This command does not prevent sending the GTD to a gatekeeper. Any GTD on the originating gateway is sent to the gatekeeper for use in routing decisions. To prevent GTD creation, the **signal-end-to-end** command-line interface (CLI) option on the R2 interfaces should be disabled, and the Cisco PGW 2200 should be configured not to send GTD to the gateway.

Examples

The following example sets unconditional signal forwarding on a system-wide basis, where the GTD payload is tunneled in H.225 SETUP messages to endpoints:

```
Router(config)# voice service voip
Router(conf-voi-serv)# signaling forward unconditional
Router(conf-voi-serv)# ^Z
Router# show running-config

Building configuration...

Current configuration : 4201 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
!
.
.
.
!
voice service voip
 signaling forward unconditional
 h323
!
.
.
.
```

Related Commands

Command	Description
clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
session target	Specifies a network-specific address for a dial peer.

signal-type

To set the signaling type to be used when connecting to a dial peer, use the **signal-type** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

signal-type {**cas** | **cept** | **ext-signal** | **transparent**}

no signal-type

Syntax Description

cas	North American EIA-464 channel-associated signaling (robbed bit signaling). If the Digital T1 Packet Voice Trunk Network Module is installed, this option might not be available.
cept	Provides a basic E1 ABCD signaling protocol. Used primarily for E&M interfaces. When used with FXS/FXO interfaces, this protocol is equivalent to MELCAS.
ext-signal	External signaling. The digital signal processor (DSP) does not generate any signaling frames. Use this option when there is an external signaling channel, for example, CCS, or when you need to have a permanent "dumb" voice pipe.
transparent	Selecting this option produces different results depending on whether you are using a digital voice module (DVM) or an analog voice module (AVM). For a DVM: The ABCD signaling bits are copied from or transported through the T1/E1 interface "transparently" without modification or interpretation. This enables the handling of arbitrary or unknown signaling protocols. For an AVM: It is not possible to provide "transparent" behavior without interpreting the signaling information to read and write the correct state to the analog hardware. This option is mapped to be equal to **cas**.

Command Default **cas**

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	The **cept** and **transparent** keywords, previously supported only on the Cisco MC3810, are now supported on the Cisco 2600 series, Cisco 3600 series, and 7200 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies to Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) dial peers. It is used with permanent connections only (Cisco trunks and FRF.11 trunks), not with switched calls.

This command is used to inform the local telephony interface of the type of signaling it should expect to receive from the far-end dial peer. To turn signaling off at this dial peer, select the **ext-signal** option. If signaling is turned off and there are no external signaling channels, a "hot" line exists, enabling this dial peer to connect to anything at the far end.

When you connect an FXS to another FXS, or if you have anything other than an FXS/FXO or E&M/E&M pair, the appropriate signaling type on Cisco 2600 and Cisco 3600 series routers is **ext-signal** (disabled).

If you have a digital E1 connection at the remote end that is running cept/MELCAS signaling and you then trunk that across to an analog port, you should make sure that you configure both ends for the **cept** signal type.

If you have a T1 or E1 connection at both ends and the T1/E1 is running a signaling protocol that is neither EIA-464, or cept/MELCAS, you might want to configure the signal type for the transparent option in order to pass through the signaling.

Examples

The following example disables signaling for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 signal-type ext-signal
 exit
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
connection	Specifies the connection mode for a voice port.
destination-pattern	Specifies the telephone number associated with a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Enables the preferred dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP.
session protocol	Establishes the VoFR protocol for calls between local and remote routers.
session target	Specifies a network-specific address for a dial peer.

silent-fax

To configure the voice dial peer for a Type 2 silent fax machine, use the **silent-fax** command in dial peer voice configuration mode. To disable a silent fax call to any POTS ports, use the **no** form of this command.

silent-fax

no silent-fax

Syntax Description This command has no arguments or keywords.

Command Default Silent fax is not configured.

Command Modes Dial peer voice configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines Use this command to configure the router to send a no ring alert tone to a Type 2 silent fax machine that is connected to any of the POTS ports. To check the status of the silent-fax configuration, use the **show running-config** command.

Examples The following example shows that the **silent-fax** command has been configured on POTS port 1 but not on POTS port 2.

```
dial-peer voice 1 pots
 destination-pattern 5551111
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 3334444 ring 1
 subaddress 20
 silent-fax

dial-peer voice 2 pots
 destination-pattern 5552222
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 3214567 ring 2
 subaddress 10
```

sip

To enter SIP configuration mode, use the **sip** command in voice-service VoIP configuration mode.

sip

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Voice-service VoIP configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines From the voice-service VoIP configuration mode, this command enables you to enter SIP configuration mode. From this mode, several SIP commands are available, such as the **bind**, **session transport**, and **url** commands.

Examples The following example enters SIP configuration mode and sets the **bind** command on the SIP network:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# bind control source-interface FastEthernet 0
```

Related Commands

Command	Description
session transport	Configures the voice dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.
voice service voip	Enters voice-service configuration mode.

sip-header

To specify the Session Initiation Protocol (SIP) header to be sent to the peer call leg, use the **sip-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

sip-header {**sip-req-uri** | *header-name*}

no sip-header {**sip-req-uri** | *header-name*}

Syntax Description

sip-req-uri	Configures Cisco Unified Border Element (UBE) to send a SIP request Uniform Resource Identifier (URI) to the peer call leg.
header-name	Name of the header to be sent to the peer call leg.

Command Default

SIP header is not sent to the peer call leg.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **sip-header** command to configure Cisco UBE to pass the unsupported parameters present in a mandatory header from one peer call leg to another of a Cisco UBE.

Examples

The following example shows how to configure Cisco UBE to send a “From” header to the peer call leg:

```
Router(config)# voice class sip-copylist 2
Router(config-class)# sip-header From
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to a peer call leg and enters voice class configuration mode.

sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode. To remove a network address configured for SIP, use the **no** form of this command.

sip-server {**dns:**[*host-name*] | **ipv4:***ipv4-address* | **ipv6:**[*ipv6-address*][**:***port-num*]}

no sip-server

Syntax Description

dns:	Sets the global SIP server interface to a Domain Name System (DNS) hostname. If you do not specify a hostname, the default DNS defined by the **ip name-server** command is used.
host-name	(Optional) Valid DNS hostname in the following format: name.gateway.xyz.
ipv4:*ipv4-address*	Sets the global SIP server interface to an IPv4 address. A valid IPv4 address takes the following format: xxx.xxx.xxx.xxx.
ipv6:[*ipv6-address*]	Sets the global SIP server interface to an IPv6 address. You must enter brackets around the IPv6 address.
:*port-num*	(Optional) Port number for the SIP server.

Command Default

No network address is configured.

Command Modes

SIP user-agent configuration (conf-serv-sip)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

If you use this command, you can also use the **session target sip-server** command on each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. Configuring a SIP server as a session target is useful if a Cisco SIP proxy server (SPS) is present in the network. With an SPS, you can configure the SIP server option and have the interested dial peers use the SPS by default.

To reset this command to a null value, use the **default** command.

To configure an IPv6 address, the user must enter brackets [ ] around the IPv6 address.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS hostname "3660-2.sip.com." If you also use the **session target sip server** command, you need not set the DNS hostname for each individual dial peer.

```
sip-ua
 sip-server dns:3660-2.sip.com

dial-peer voice 29 voip
 session target sip-server
```

The following example sets the global SIP server interface to an IPv4 address:

```
sip-ua
 sip-server ipv4:10.0.2.254
```

The following example sets the global SIP server interface to an IPv6 address. Note that brackets were entered around the IPv6 address:

```
sip-ua
 sip-server ipv6:[2001:0DB8:0:0:8:800:200C:417A]
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
session target (VoIP dial peer)	Specifies a network-specific address for a dial peer.
session target sip-server	Instructs the dial peer session target to use the global SIP server.
sip-ua	Enters SIP user-agent configuration mode in order to configure the SIP user agent.

sip-ua

To enable Session Initiation Protocol (SIP) user-agent configuration commands, in order to configure the user agent, use the **sip-ua** command in global configuration mode. To reset all SIP user-agent configuration commands to their default values, use the **no** form of this command.

sip-ua

no sip-ua

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, no SIP user-agent configuration commands can be entered.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
15.1(2)T	The **connection-reuse** SIP user-agent configuration mode command was added.

Usage Guidelines

Use this command to enter SIP user-agent configuration mode. Table 230 lists the SIP user-agent configuration mode commands.

Table 230 SIP User-Agent Configuration Mode Commands

Command	Description
connection-reuse	Uses the listener port for sending requests over the User Datagram Protocol (UDP).
exit	Exits SIP user-agent configuration mode.
inband-alerting	This command is no longer supported as of Cisco IOS Release 12.2 because the gateway handles remote or local ringback on the basis of SIP messaging.
max-forwards	Specifies the maximum number of hops for a request.

Table 230 SIP User-Agent Configuration Mode Commands (continued)

Command	Description
retry	Configures the SIP signaling timers for retry attempts.
sip-server	Configures a SIP server interface.
timers	Configures the SIP signaling timers.
transport	Enables or disables a SIP user agent transport for TCP or UDP that the protocol SIP user agents listen for on port 5060 (default).

Examples

The following example, beginning in global configuration mode, shows how to enter SIP user-agent configuration mode, configure the SIP user agent, and then return to global configuration mode:

```
Router# sip-ua
Router(sip-ua)# retry invite 2
Router(sip-ua)# retry response 2
Router(sip-ua)# retry bye 2
Router(sip-ua)# retry cancel 2
Router(sip-ua)# sip-server ipv4:10.0.2.254
Router(sip-ua)# timers invite-wait-100 500
Router(sip-ua)# exit
Router#
```

Related Commands

Command	Description
exit	Exits SIP user-agent configuration mode.
max-forwards	Specifies the maximum number of hops for a request.
retry	Configures the retry attempts for SIP messages.
show sip-ua	Displays statistics for SIP retries, timers, and current listener status.
sip-server	Configures the SIP server interface.
timers	Configures the SIP signaling timers.
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

snmp enable peer-trap poor-qov

To generate poor-quality-of-voice notifications for applicable calls associated with VoIP dial peers, use the **snmp enable peer-trap poor-qov** command in dial peer configuration mode. To disable notification, use the **no** form of this command.

snmp enable peer-trap poor-qov

no snmp enable peer-trap poor-qov

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

Use this command to generate poor-quality-of-voice notification for applicable calls associated with a dial peer. If you have a Simple Network Management Protocol (SNMP) manager that uses SNMP messages when voice quality drops, you might want to enable this command. Otherwise, you should disable this command to reduce unnecessary network traffic.

Examples

The following example enables poor-quality-of-voice notification for calls associated with VoIP dial peer 10:

```
dial-peer voice 10 voip
 snmp enable peer-trap poor-qov
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and information.
snmp trap link-status	Enables SNMP trap messages to be generated when a specific port is brought up or down.

soft-offhook

To enable stepped off-hook resistance during seizure, use the **soft-offhook** command in voice-port (FXO) configuration mode. To disable this command, use the **no** form of this command.

soft-offhook

no soft-offhook

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, which means there is no stepped off-hook resistance during seizure.

Command Modes

Voice-port (FXO) configuration (config-voiceport)

Command History

Release	Modification
12.4(3f) 12.4(4)T4	This command was introduced.

Usage Guidelines

An off-hook indication into a far-end ringing cadence ON condition can occur during glare conditions (outgoing seizure occurring at the same time as an incoming ring). This condition can also occur when the interface configuration includes the **connection plar-opx** command. If the **connection plar-opx** command is not configured, the FXO software waits for a ringing cadence to transition from ON to OFF prior to transitioning to the off-hook condition. (Glare can be minimized by configuring ground-start signaling.)

When the **soft-offhook** command is entered, the FXO hookswitch off-hook resistance is initially set to a midresistance value for outgoing or incoming seizure. This resistance limits the ringing current that occurs during seizure into ringing signals prior to far-end ring-trip. When ringing is no longer detected, hookswitch resistance is returned to its normal lower value. This prevents damage to the FXO line interface that may occur in locations with short loops and conventional ringing sources with low output impedance ringing sources that have the potential to deliver high current.

The **soft-offhook** command applies to the following FXO interface cards (which use the 3050i chipset):

- EM-HDA-3FXS/4FXO (EVM-HD-8FXS/DID, FXO ports only)
- EM-HDA-6FXO (on EVM-HD-8FXS/DID)
- EM2-HDA-4FXO (NM-HDA-4FXS network module only)
- VIC2-4FXO, VIC2-2FXO

Examples

The following example shows a sample configuration session to enable stepped off-hook resistance during seizure on voice port 1/0/0 on a Cisco 3725 router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# voice-port 1/0/0
Router(config-voiceport)# soft-offhook
Router(config-voiceport)# shutdown
Router(config-voiceport)#
Nov  3 11:08:53.313 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
state to Administrative Shutdown

Router(config-voiceport)# no shutdown
Router(config-voiceport)#
Nov  3 11:08:58.290 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
state to up

Router(config-voiceport)# ^Z
Router#
Nov  3 11:09:01.086 EST: %SYS-5-CONFIG_I: Configured from console by console

Router#
```

Related Commands

Command	Description
connection plar-opx	Specifies the connection mode for a voice port as PLAR-OPX.
voice-port	Enters voice-port configuration mode.

source carrier-id

To configure debug filtering for the source carrier ID, use the **source carrier-id** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source carrier-id *string*

no source carrier-id *string*

Syntax Description

string	Alphanumeric identifier for the carrier ID.

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match source carrier ID 4321:

```
call filter match-list 1 voice
 source carrier-id 4321
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source trunk-group-label	Configure debug filtering for a source trunk group.
target carrier-id	Configure debug filtering for the target carrier ID.
target trunk-group-label	Configure debug filtering for a target trunk group.

source trunk-group-label

To configure debug filtering for a source trunk group, use the **source trunk-group-label** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source trunk-group-label *group_number*

no source trunk-group-label *group_number*

Syntax Description

group_number	A value from 0 to 23 that identifies the trunk group.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match source trunk group 21:

```
call filter match-list 1 voice
 source trunk-group-label 21
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source carrier-id	Configure debug filtering for the source carrier ID.
target carrier-id	Configure debug filtering for the target carrier ID.
target trunk-group-label	Configure debug filtering for a target trunk group.

speed dial

To designate a range of digits for SCCP telephony control (STC) application feature speed-dial codes, use the **speed dial** command in STC application feature speed-dial configuration mode. To return the range to its default, use the **no** form of this command.

speed dial from *digit* **to** *digit*

no speed dial

Syntax Description

from *digit*	Starting number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 1 for one-digit codes; 01 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.
to *digit*	Ending number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 9 for one-digit codes; 99 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.

Command Default

The default speed-dial codes are 1 to 9 for one-digit codes; 01 to 99 for two-digit codes.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	The *digit* argument was modified to allow two-digit codes.

Usage Guidelines

This command is used with the STC application, which enables features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Use this command to set the range of speed-dial codes only if you want to change the range from its default. The **digit** command determines whether speed-dial codes are one-digit or two-digit.

A maximum of nine one-digit or 99 two-digit speed-dial codes are supported. If you set the starting number to 0, the highest number you can set for the ending number is 8 for one-digit codes, or 98 for two-digit codes.

Note that the actual telephone numbers that are speed dialed are stored on Cisco CallManager or the Cisco CallManager Express system. The speed-dial codes that you set with this command are mapped to speed-dial positions on the call-control device. For example, if you set the starting number to 2 and the ending number to 7, the system maps 2 to speed-dial 1 and maps 7 to speed-dial 6.

You can enter numbers in this command in ascending or descending order. For example, the following commands are both valid:

```
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# speed dial from 7 to 2
```

To use the speed-dial feature on a phone, dial the STC application feature speed-dial (FSD) prefix and one of the speed-dial codes that has been configured with this command (or the default if this command was not used). For example, if the FSD prefix is * (the default) and the speed-dial codes are 1 to 9 (the default), dial *3 to dial the telephone number stored with speed-dial 3.

This command resets to its default range if you modify the value of the **digit** command. For example, if you set the **digit** command to 2, then change the **digit** command back to its default of 1, the speed-dial codes are reset to 1 to 9.

If the **digit** command is set to 2 and you configure a single-digit speed-dial code, the system converts the speed-dial code to two digits. For example, if you enter the range 1 to 5 in a two-digit configuration, the system converts the speed-dial codes to 11 to 15.

If you set any of the FSD codes in this range to a value that is already in use for another FSD code, you receive a warning message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

The **show running-config** command displays nondefault FSD codes only. The **show stcapp feature codes** command displays all FSD codes.

Examples

The following example sets an FSD code prefix of two pound signs (##) and a speed-dial code range of 2 to 7. After these values are configured, a phone user presses ##2 to dial the number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ##
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

```
Router# show stcapp feature codes
.
.
.
  stcapp feature speed-dial
    prefix ##
    redial ###
    speeddial number of digit(s) 1
    voicemail ##0
    speeddial1 ##2
    speeddial2 ##3
    speeddial3 ##4
    speeddial4 ##5
    speeddial5 ##6
    speeddial6 ##7
```

The following example sets a FSD code prefix of two asterisks (**) and a speed-dial code range of 12 to 17.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix **
Router(stcapp-fsd)# digit 2
Router(stcapp-fsd)# speed dial from 12 to 17
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for STC application feature speed-dial codes.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature access codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

srtp (dial peer)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls for a specific VoIP dial peer, to enable fallback, and to override global SRTP configuration, use the **srtp** command in dial peer voice configuration mode. To disable secure calls, to disable fallback, and to override global SRTP configuration, use the **no** form of this command.

srtp [**fallback** | **system**]

no srtp [**fallback** | **system**]

Syntax Description

fallback	(Optional) Enables specific dial-peer calls to fall back to nonsecure mode.
system	(Optional) Enables the global SRTP configuration that was set using the **srtp** command in voice service voip configuration mode. This is the default if the **srtp** command is enabled in dial peer voice configuration mode.

Command Default

Global SRTP configuration set in voice service voip configuration mode is enabled.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(6)T1	This command was introduced.

Usage Guidelines

You can enable secure calls using the **srtp** command either at the dial peer level, or at the global level. The **srtp** command in dial peer voice mode configures call security at the dial-peer level and takes precedence over the global **srtp** command. Use the **srtp** command in dial peer voice configuration mode to enable secure calls for a specific dial peer. Use the **no** form of this command to disable secure calls.

Use the **srtp fallback** command to enable secure calls and allow calls to fallback to nonsecure mode for a specific dial peer. This security policy applies to all calls going through the dial peer and is not configurable on a per-call basis. Using the **srtp fallback** command to configure call fallback at the dial-peer level takes precedence over the global **srtp fallback** command. The **no** form of this command disables SRTP and fallback. If you disallow fallback using the **no srtp fallback** command, a call cannot fall back to nonsecure mode.

Use the **srtp system** command to apply global level security settings to dial peers.

Examples

The following example enables secure calls and disallows fallback for a specific dial peer:

```
Router(config-dial-peer)# srtp
```

The following example enables secure calls and allows call fallback to nonsecure mode:

```
Router(config-dial-peer)# srtp fallback
```

The following example defaults call security to global level SRTP behavior:

```
Router(config-dial-peer)# srtp system
```

Related Commands

Command	Description
srtp (voice)	Enables secure calls globally in voice service voip configuration mode.
srtp fallback (voice)	Enables SRTP and fallback globally.

srtp (voice)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls and call fallback, use the **srtp** command in voice service voip configuration mode. To disable secure calls and disallow fallback, use the **no** form of this command.

srtp [**fallback**]

no srtp [**fallback**]

Syntax Description

fallback	(Optional) Enables call fallback to nonsecure mode.

Command Default

Voice call security and fallback are disabled.

Command Modes

Voice service voip configuration

Command History

Release	Modification
12.4(6)T1	This command was introduced.

Usage Guidelines

Use the **srtp** command in voice service voip configuration mode to globally enable secure calls using SRTP media authentication and encryption. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial peer voice configuration mode. Using the **srtp** command to configure call security at the dial-peer level takes precedence over the global **srtp** command.

Use the **srtp fallback** command to globally enable secure calls and allow calls to fall back to RTP (nonsecure) mode. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial peer voice configuration mode. Using the **srtp fallback** command in dial peer voice configuration mode to configure call security takes precedence over the **srtp fallback** global command in voice service voip configuration mode. If you use the **no srtp fallback** command, fallback from SRTP to RTP (secure to nonsecure) is disallowed.

Examples

The following example enables secure calls:

```
Router(config-voi-serv)# srtp
```

The following example enables call fallback to nonsecure mode:

```
Router(config-voi-serv)# srtp fallback
```

Related Commands

Command	Description
srtp (dial peer)	Enables secure calls on an individual dial peer.
srtp fallback (dial peer)	Enables call fallback to RTP (nonsecure) mode on an individual dial peer.
srtp fallback (voice)	Enables call fallback globally to RTP (nonsecure) mode.
srtp system	Enables secure calls on a global level.

srv version

To generate Domain Name System Server (DNS SRV) queries with either the RFC 2052 or RFC 2782 format, use the **srv version** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

srv version {**1** | **2**}

no srv version

Syntax Description

1	Specifies the domain-name prefix of format protocol.transport. (RFC 2052 style).
2	Specifies the domain-name prefix of format _protocol._transport. (RFC 2782 style).

Defaults

2 (RFC 2782 style)

Command Modes

SIP UA configurationn (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5850 in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses DNS SRV queries to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." (RFC 2052) or "_protocol._transport." (RFC 2782). The selected string is then attached to the fully qualified domain name (FQDN) of the next hop SIP server.

By configuring the value of 1, this command provides compatibility with older equipment that supports only RFC 2052.

Examples

The following example sets up the **srv version** command in the RFC 2782 style (underscores surrounding the protocol):

```
Router(config)# sip-ua
Router(config-sip-ua)# srv version 2
```

Related Commands

Command	Description
show sip-ua status	Displays SIP status.

ss7 mtp2-variant

To configure a Signaling System 7 (SS7) signaling link, use the **ss7 mtp2-variant** command in global configuration mode. To restore the designated default, use the **no** form of this command.

ss7 mtp2-variant [**bellcore** *channel* | **itu-white** *channel* | **ntt** *channel* | **ttc** *channel*] [*parameters*]

no ss7 mtp2-variant

Syntax Description

bellcore	Configures the router for Telcordia Technologies (formerly Bellcore) standards.
channel	Message Transfer Part Layer 2 (MTP2) serial channel number. Range is from 0 to 3.
itu-white	Configures the SS7 channel with the ITU-white protocol variant.
ntt	Configures the router for NTT (Japan) standards. **Note** This keyword is not available with the PCR feature.
ttc	Configures the router for Japanese Telecommunications Technology Committee (TTC) standards. **Note** This keyword is not available with the PCR feature.
parameters	(Optional) Configures a particular standard. See Table 231, Table 232, Table 233, and Table 234 in the "Usage Guidelines" section for accepted parameters.

Command Default

bellcore

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	This command was modified to include all possible variants: **bellcore**, **itu-white**, **ntt**, **ttc**.

Usage Guidelines

Note When the **bellcore** or **itu-white** variant is selected, this command enters a new configuration mode for setting MTP2 parameters: ITU configuration mode. See the **error-correction** command reference for information about setting MTP2 parameters from this mode.

The MTP2 variant has timers and parameters that can be configured using the values listed in the following tables. To restore the designated default, use the **no** or the **default** form of the command (see the "Examples" section below).

Table 231 Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	1600	1000 to 65535
T4-Normal-Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending status indication busy (SIB) timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535
lssu-len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
unacked-MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet-counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tie-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Table 232 ITU-white Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4-Normal-Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535

Table 232 ITU-white Parameters and Values (continued)

Parameter	Description	Default	Range
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu-len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
msu-len	message signal unit (MSU) length	1	1 to 2
unacked-MSUs	Maximum number of MSUs awaiting acknowledgment (ACK)	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Table 233 NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	Fill-in Signal Unit (FISU) interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked-MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal Unit Error Rate Monitor (SUERM) e error-rate threshold	64	32 to 128

Table 233 NTT Parameters and Values (continued)

Parameter	Description	Default	Range
SUERM-number -octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal Unit Error Rate Monitor (SUERM) units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8

Table 234 TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked-MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal -units	Signal units (good or bad) needed to decrement ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example configures an SS7 channel (link) for Preventive Cyclic Retransmission (PCR) with forced retransmission initiated. In this example, SS7 channel 0 is configured with the ITU-white protocol variant using the PCR error correction method.

```
Router# configure terminal
Router(config)# ss7 mtp2-variant itu-white 0
```

```
Router(config-ITU)# error-correction pcr forced-retransmission enabled N2 1000
Router(config-ITU)# end
```

The following example disables error-correction:

```
Router(config-ITU)# no error-correction
```

Related Commands

Command	Description
error-correction	Sets the error correction method for the SS7 signaling link when the SS7 MTP2 variant is Bellcore or ITU-white.
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

ss7 mtp2-variant bellcore

To configure the router for Telcordia Technologies (formerly Bellcore) standards, use the **ss7 mtp2-variant bellcore** command in global configuration mode.

ss7 mtp2-variant bellcore [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See Table 235 for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured.
See Table 235 for default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This MTP2 variant has timers and parameters that can be configured using the values listed in Table 235. To restore the designated default, use the **no** or the **default** form of the command (see example below).

Note Timer durations are converted to 10-millisecond units. For example, a T1 value of 1005 is converted to 100, which results in an actual timeout duration of 1000 ms. This is true for all timers and all variants.

Table 235 Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	600	1000 to 65535
T4-Normal-Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535
lssu-len	1- or 2-byte LSSU format	1	1 to 2

Table 235 Bellcore (Telcordia Technologies) Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error-rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet-counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tie-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the aligned/ready timer duration on channel 0 to 30,000 ms:

```
ss7 mtp2-variant bellcore 0 T1 30000
```

The following example restores the aligned/ready timer default value of 13,000 ms:

```
ss7 mtp2-variant bellcore 0 no T1
```

Related Commands

Command	Description
ss7 mtp2-variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2-variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant itu

To configure the router for ITU (International Telecom United) standards, use the **ss7 mtp2-variant itu** command in global configuration mode.

ss7 mtp-variant itu [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See Table 236 for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured.
See Table 236 for ITU default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in Table 236. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 236 ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4-Normal-Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu-len	1- or 2-byte LSSU format	1	1 to 2
msu-len			

Table 236 ITU (White) Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the emergency proving period on channel 1 to 10,000 ms:

```
ss7 mtp2-variant itu 1
 t4-Emergency-Proving 10000
```

The following example restores the emergency proving period default value of 5,000 ms:

```
ss7 mtp2-variant itu 1
 default t4-Emergency-Proving
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ntt

To configure the router for NTT (Japan) standards, use the **ss7 mtp2-variant ntt** command in global configuration mode.

ss7 mtp-variant ntt [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See Table 237 for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured.
See Table 237 for NTT default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The NTT MTP2 variant has timers and parameters that can be configured using the values listed in Table 237. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 237 NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Table 237 NTT Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the SUERM error rate threshold on channel 2 to 100:

```
ss7 mtp2-variant ntt 2
 SUERM-threshold 100
```

The following example restores the SUERM error rate threshold default value of 64:

```
ss7 mtp2-variant ntt 2
 no SUERM-threshold
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ttc

To configure the router for TTC (Japan Telecom) standards, use the **ss7 mtp2-variant ttc** command in global configuration mode.

ss7 mtp-variant ttc [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See Table 238 for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured.
See Table 238 for TTC default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The TTC MTP2 variant has timers and parameters that can be configured using the values listed in Table 238. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 238 TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Table 238 TTC Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	SUERM error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie-AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the maximum number of proving attempts for channel 3 to 3:

```
ss7 mtp2-variant ttc 3
 proving-attempts 3
```

The following example restores the maximum number of proving attempts to the default value:

```
ss7 mtp2-variant ttc 3
 default proving-attempts
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2-variant ntt	Specifies the MTP2-variant as NTT.

ss7 mtp2-variant itu-white

To configure the router for International Telecommunications Union (ITU) standards, use the **ss7 mtp2-variant itu-white** command in global configuration mode.

ss7 mtp2-variant itu-white [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Message Transfer Part 2 (MTP2) serial channel number. The range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See Table 236 for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured.
See Table 236 for ITU default parameters.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in Table 236. To restore the designated default, use the **no** or the **default** form of the command.

Table 239 ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds [ms])	40000	1000 to 65535
T2	Not aligned timer (ms)	5000	1000 to 65535
T3	Aligned timer (ms)	1000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (ms)	500	1000 to 65535
T4-Normal-Proving	Normal proving timer (ms)	8200	1000 to 65535
T5	Sending SIB timer (ms)	100	80 to 65535
T6	Remote congestion timer (ms)	6000	1000 to 65535
T7	Excessive delay timer (ms)	1000	1000 to 65535
lssu-len	1- or 2-byte Links Status Signal Unit (LSSU) format	1	1 to 2
msu-len	—	—	—

Table 239 ITU (White) Parameters and Values (continued)

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of Message Signal Units (MSUs) waiting acknowledgement	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal unit error monitor (SUERM) error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal-units	Signal units (good or bad) needed to dec Embedded Resource Manager (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Unit Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example shows how to set the emergency proving period on channel 1 to 10,000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# t4-Emergency-Proving 10000
```

The following example shows how to restore the emergency proving period default value of 5000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# default t4-Emergency-Proving 5000
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2 variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2 variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2 variant as TTC.

ss7 session

To create a Reliable User Datagram Protocol (RUDP) session and explicitly add an RUDP session to a Signaling System 7 (SS7) session set, use the **ss7 session** command in global configuration mode. To delete the session, use the **no** form of this command.

ss7 session *session-id* **address** *destination-address destinaion-port local-address local-port* [**session-set** *session-number*]

no ss7 session *session-id*

Syntax Description

session-id	SS7 session number. Valid values are 0 and 1. You must enter a hyphen with no space following it after the **session** keyword.
address *destination-address*	Specifies the SS7 session IP address.
destination-address	The local IP address of the router in four-part dotted-decimal format. The local IP address for both sessions, 0 and 1, must be the same.
destination-port	The number of the local UDP port on which the router expects to receive messages from the media gateway controller (MGC). Specify any UDP port that is not used by another protocol as defined in RFC 1700 and that is not otherwise used in your network. The local UDP port must be different for session 0 and session 1. Valid port ranges are from 1024 to 9999.
local-address	The remote IP address of the MGC in four-part dotted-decimal format.
local-port	The number of the remote UDP port on which the MGC is configured to listen. This UDP port cannot be used by another protocol as defined in RFC 1700 and cannot be otherwise used in the network. Valid port ranges are from 1024 to 9999.
session-set session-number	(Optional) Assigns an SS7 session to an SS7 session set.

Command Default

No session is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(15)T	The **session-set** keyword and the *session-number* argument were added.

Usage Guidelines

For the Cisco 2600-based SLT, you can configure a maximum of four sessions, two for each Cisco SLT. In a redundant VSC configuration, session 0 and session 2 are configured to one VSC, and session 1 and session 3 are configured to the other. Session 0/1 and session 2/3 run to the Cisco SLT.

The VSC must be configured to send messages to the local port, and it must be configured to listen on the remote port. You must also reload the router whenever you remove a session or change the parameters of a session.

This command replaces the **ss7 session-0 address** and **ss7 session-1 address** commands, which contain hard-coded session numbers. The new command is used for the new dual Ethernet capability.

The new CLI supports both single and dual Ethernet configuration by being backward compatible with the previous **session-0** and **session-1** commands so that you can configure a single Ethernet instead of two, if needed.

For the Cisco AS5350 and Cisco AS5400-based SLT, you can configure a maximum of two sessions, one for each signaling link. In a redundant MGC configuration, session 0 is configured to one MGC and session 1 is configured to the other.

The MGC must be configured to send messages to the local port, and the MGC must be configured to listen on the remote port.

You must reload the router whenever you remove a session or change the parameters of a session.

By default, each RUDP session must belong to SS7 session set 0. This allows backward compatibility with existing SS7 configurations.

If the **session-set** keyword is omitted, the session is added to the default SS7 session set 0. This allows backward compatibility with older configurations. Entering the **no** form of the command is still sufficient to remove the session ID for that RUDP session.

If you want to change the SS7 session set to which a session belongs, you have to remove the entire session first. This is intended to preserve connection and recovery logic.

Examples

The following example sets up two sessions on a Cisco 2611 and creates session set 2:

```
ss7 session-0 address 172.16.1.0 7000 172.16.0.0 7000 session-set 2
ss7 session-1 address 172.17.1.0 7002 172.16.0.0 7001 session-set 2
```

Note The example above shows how the local IP addresses in session-0 and session-1 must be the same.

Related Commands

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.

ss7 session cumack_t

To set the Reliable User Datagram Protocol (RUDP) cumulative acknowledgment timer for a specific SS7 signaling link session, use the **ss7 session cumack_t** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **cumack_t** *milliseconds*

no ss7 session-*session number* **cumack_t**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the RUDP waits before it sends an acknowledgment after receiving a segment. Range is from 100 to 65535. The value should be less than the value configured for the retransmission timer by using the **ss7 session**-*session number* **retrans_t** command.

Command Default

300 ms

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The cumulative acknowledgment timer determines when the receiver sends an acknowledgment. If the timer is not already running, it is initialized when a valid data, null, or reset segment is received. When the cumulative acknowledgment timer expires, the last in-sequence segment is acknowledged. The RUDP typically tries to "piggyback" acknowledgments on data segments being sent. However, if no data segment is sent in this period of time, it sends a standalone acknowledgment.

Examples

The following example sets up two sessions and sets the cumulative acknowledgment timer to 320 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 cumack_t 320
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 cumack_t 320
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session kp_t

To set the null segment (keepalive) timer for a specific SS7 signaling link session, use the **ss7 session kp_t** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **kp_t** *milliseconds*

no ss7 session-*session number* **kp_t**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the Reliable User Datagram Protocol (RUDP) waits before sending a keepalive to verify that the connection is still active. Valid values are 0 and from100 to 65535. Default is 2000.

Command Default 2000 ms

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines The null segment timer determines when a null segment (keepalive) is sent by the client Cisco 2600 series router. On the client, the timer starts when the connection is established and is reset each time a data segment is sent. If the null segment timer expires, the client sends a keepalive to the server to verify that the connection is still functional. On the server, the timer restarts each time a data or null segment is received from the client.

The value of the server's null segment timer is twice the value configured for the client. If no segments are received by the server in this period of time, the connection is no longer valid.

To disable keepalive, set this parameter to 0.

Examples The following example sets up two sessions and sets a keepalive of 1,800 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 kp_t 1800
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 kp_t 1800
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_cumack

To set the maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_cumack** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **m_cumack** *segments*

no ss7 session-*session number* **m_cumack**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment. Range is from 0 to 255. Default is 3.

Command Default 3 segments

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines The cumulative acknowledgment counter records the number of unacknowledged, in-sequence data, null, or reset segments received without a data, null, or reset segment being sent to the transmitter. If this counter reaches the configured maximum, the receiver sends a standalone acknowledgment (a standalone acknowledgment is a segment that contains only acknowledgment information). The standalone acknowledgment contains the sequence number of the last data, null, or reset segment received.

If you set this parameter to 0, an acknowledgment is sent immediately after a data, null, or reset segment is received.

Examples The following example sets up two sessions and in each session sets a maximum of two segments for receipt before acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
```

```
ss7 session-0 m_cumack 2
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_cumack 2
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_outseq

To set the maximum number of out-of-sequence segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an extended acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_outseq** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **m_outseq** *segments*

no ss7 session-*session number* **m_outseq**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment. If the specified number of segments are received out of sequence, an Extended Acknowledgment segment is sent to inform the sender which segments are missing. Range is from 0 to 255. Default is 3.

Command Default 3 segments

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines The out-of-sequence acknowledgment counter records the number of data segments that have arrived out of sequence. If this counter reaches the configured maximum, the receiver sends an extended acknowledgment segment that contains the sequence numbers of the out-of-sequence data, null, and reset segments received. When the transmitter receives the extended acknowledgment segment, it retransmits the missing data segments.

If you set this parameter to 0, an acknowledgment is sent immediately after an out-of-sequence segment is received.

Examples The following example sets up two sessions and sets a maximum number of four out-of-sequence segments for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_outseq 4
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_outseq 4
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_rcvnum

To set the maximum number of segments that the remote end can send before receiving an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_rcvnum** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **m_rcvnum** *segments*

no ss7 session-*session number* **m_rcvnum**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that the remote (Cisco IOS software) end can send before receiving an acknowledgment. Range is from 1 to 64. Default is 32.

Command Default 32 segments

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines The outstanding segments counter is the maximum number of segments that the Cisco IOS software end of the connection can send without getting an acknowledgment from the receiver. The receiver uses the counter for flow control.

Examples The following example sets up two sessions and for each session sets a maximum of 36 segments for receipt before an acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_rcvnum 36
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_rcvnum 36
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_retrans	Sets the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session m_retrans

To set the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid in a specific SS7 signaling link session, use the **ss7 session m_retrans** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **m_retrans** *number*

no ss7 session-*session number* **m_retrans**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
number	Maximum number of times that the RRUDP attempts to resend a segment before declaring the connection broken. Range is from 0 to 255. Default is 2.

Command Default

2 times

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The retransmission counter is the number of times a segment has been retransmitted. If this counter reaches the configured maximum, the transmitter resets the connection and informs the upper-layer protocol.

If you set this parameter to 0, the RUDP attempts to resend the segment continuously.

Examples

The following example sets up two sessions and for each session sets a maximum number of three times to resend before a session becomes invalid:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_retrans 3
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_retrans 3
```

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
show ss7	Displays the SS7 configuration.

ss7 session retrans_t

To set the amount of time that the Reliable User Datagram Protocol (RUDP) waits to receive an acknowledgment for a segment in a specific SS7 signaling link session, use the **ss7 session retrans_t** command in global configuration mode. If the RUDP does not receive the acknowledgment in this time period, the RUDP retransmits the segment. To reset to the default, use the **no** form of this command.

ss7 session-*session number* **retrans_t** *milliseconds*

no ss7 session-*session number* **retrans_t**

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Amount of time, in milliseconds, that the RUDP waits to receive an acknowledgment for a segment. Range is from 100 to 65535. Default is 600.

Command Default

600 ms

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The retransmission timer is used to determine whether a packet must be retransmitted and is initialized each time a data, null, or reset segment is sent. If an acknowledgment for the segment is not received by the time the retransmission timer expires, all segments that have been transmitted—but not acknowledged—are retransmitted.

This value should be greater than the value configured for the cumulative acknowledgment timer by using the **ss7 session cumack_t** command.

Examples

The following example sets up two sessions and specifies 550 ms as the time to wait for an acknowledgment for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 retrans_t 550
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 retrans_t 550
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.

ss7 set

Note Effective with Cisco IOS Release 12.2(15)T, the **ss7 set** command replaces the **ss7 set failover-timer** command.

To independently select failover-timer values for each session set and to specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session, use the **ss7 set** command in global configuration mode. To restore the restore the failover timer to its default value of 5, use the **no** form of this command.

ss7 set [**session-set** *session-id*] **failover-timer** *ft-value*

no ss7 set [**session-set** *session-id*] **failover-timer**

Syntax Description

session-set *session-id*	(Optional) Selects failover timer values for each SS7 session set. Valid values are from 1 to 5. Default is 0.
failover-timer *ft-value*	Time, in seconds, that the Session Manager waits for a session to recover. Valid values range from 1 to 10. Default is 5.

Command Default

The failover timer is not set.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced. This command replaces the **ss7 set failover-timer** command.

Usage Guidelines

The **failover-timer** keyword and the *ft-value* argument specify the number of seconds that the Session Manager waits for the active session to recover or for the standby MGC to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the failover timer expires without recovery of the original session or if the system fails to get an active message from the standby MGC, the signaling links are taken out of service.

The **no** form of this command restores the failover timer to its default value of 5. Omitting the optional **session-set** keyword implicitly selects SS7 session set 0, which is the default.

Examples

The following example sets the failover timer to four seconds without using the **session-set** option:

```
ss7 set failover-timer 4
```

The following example sets the failover timer to 10 seconds and sets the SS7 session set value to 5:

```
ss7 set session-set 5 failover-timer 10
```

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

ss7 set failover-timer

To specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby Media Gateway Controller to indicate that the SLT should switch traffic to the standby session, use the **ss7 set failover-timer** command in global configuration mode. To reset ti the default, use the **no** form of this command.

ss7 set failover-timer [*seconds*]

no ss7 set failover-timer

Syntax Description

seconds	Time, in seconds, that the session manager waits for a session to recover. Range is from 1 to 10. Default is 3.

Command Default 3 seconds

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines This command specifies the number of seconds that the session manager waits for the active session to recover or for the standby media gateway controller to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the timer expires without a recovery of the original session or an active message from the standby media gateway controller, the signaling links are taken out of service.

Examples The following example sets the failover timer to 4 seconds:

```
ss7 set failover-timer 4
```

Related Commands

Command	Description
show ss7 sm set	Displays the current failover timer setting.
ss7 session	Establishes a session.

station-id name

To specify the name that is to be sent as caller ID information and to enable caller ID, use the **station-id name** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the name, use the **no** form of this command.

station-id name *name*

no station-id name *name*

Syntax Description

name	Station-id name. Must be a string of 1 to 15 characters.

Defaults

The default is no station-id name.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

Do not use this command when the caller ID standard is dual-tone multifrequency (DTMF). DTMF caller ID can carry only the calling number.

If the **station-id name**, **station-id number**, or a **caller-id alerting** command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable** command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
 station-id number 4085550111

Router(config-voiceport)#station-id ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller-id enable	Enables caller ID operation.
station-id number	Enables caller ID operation and specifies the number sent from the originating station-id or network FXO port for caller ID purposes.

station-id number

To specify the telephone or extension number that is to be sent as caller ID information and to enable caller ID, use the **station-id number** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the number, use the **no** form of this command.

station-id number *number*

no station-id number *number*

Syntax Description

number	Station-id number. Must be a string of 1 to 15 characters.

Defaults

The default is no station-id number.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Within the network, if an originating station-id does not include configured number information, Cisco IOS software determines the number by using reverse dial-peer search.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

If the **station-id name**, **station-id number**, or a **caller-id alerting** command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable** command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
 station-id number 4085550111

Router(config-voiceport)#station-id ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller-id enable	Enables caller ID operation.
station-id name	Enables caller ID operation and specifies the name sent from the originating station-id or network FXO port for caller ID purposes.

stats

To enable statistics collection for voice applications, use the **stats** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

stats

no stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application stats** command.

Usage Guidelines

To display the application statistics, use the **show call application session-level**, **show call application app-level**, or **show call application gateway-level** command. To reset the application counters in history to zero, use the **clear call application stats** command.

Examples

The following example enables statistics collection for voice applications:

```
application
monitor
stats
```

Related Commands

Command	Description
call application interface stats	Enables statistics collection for application interfaces.
call application stats	Enables statistics collection for voice applications.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
interface stats	Enables statistics collection for application interfaces.
show call application app-level	Displays application-level statistics for voice applications.

Command	Description
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.

stcapp

To enable the SCCP Telephony Control Application (STCAPP), use the **stcapp** command in global configuration mode. To disable the STCAPP, use the **no** form of this command.

stcapp

no stcapp

Syntax Description This command has no arguments or keywords.

Command Default The Cisco CallManager does not control Cisco IOS gateway-connected analog and BRI endpoints.

Command Modes Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines Use the **stcapp** command to enable basic Skinny Client Call Control (SCCP) call control features for BRI and foreign exchange stations (FXS) analog ports within Cisco IOS voice gateways. The **stcapp** command enables the Cisco IOS gateway application to support the following features:

- Line-side support for the Multilevel Precedence and Preemption (MLPP) feature
- Cisco CallManager registration of analog and Basic Rate Interface BRI endpoints
- Cisco CallManager endpoint autoconfiguration support
- Modem pass-through support
- Cisco Survivable Remote Site Telephony (SRST) support

Examples The following example shows that STCAPP is enabled:

```
Router(config)# stcapp
```

Related Commands

Command	Description
ccm-manager config server	Specifies the TFTP server for SCCP gateway downloads.
ccm-manager sccp local	Specifies the SCCP local interface for Cisco CallManager registration.
sccp	Enables the SCCP protocol.
show stcapp device	Displays configuration information about STCAPP) voice ports.
show stcapp statistics	Displays call statistics for STCAPP voice ports.

Command	Description
stcapp ccm-group	Configures the Cisco CallManager group number for use by the STCAPP.
stcapp timer	Enables STCAPP timer configuration.

stcapp call-control mode

To configure call control mode for Skinny Client Control Protocol (SCCP) gateway supplementary features, use the **stcapp call-control mode** command in global configuration mode. To disable call control mode, use the **no** form of this command

stcapp call-control mode [**feature** | **standard**]

no stcapp call-control mode [**feature** | **standard**]

Syntax Description

feature	(Optional) Feature mode call control.
standard	(Optional) Standard mode call control. This is the default.

Command Default

Standard mode call control is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

This command enables feature mode call control, which allows SCCP analog phone users to invoke a feature by dialing a feature access code (FAC). The following table lists the features and FACs that you can use in feature mode.

Feature	FAC
Drop Last Active Call	#1
Call Transfer	#2
Call Conference	#3
Drop Last Conferee	#4
Toggle Between Two Calls	#5

Examples

The following partial output from the **show running-config** command shows feature call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode feature
!
```

The following partial output from the **show running-config** command shows standard call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode standard
!
!
```

Related Commands

Command	Description
show stcapp feature codes	Displays current values for SCCP telephony control (STC) application feature access codes.

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback

no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application.

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp ccm-group

To configure the Cisco CallManager group number for use by the SCCP Telephony Control Application (STCAPP), use the **stcapp ccm-group** command in global configuration mode. To disable STCAPP Cisco CallManager group number configuration, use the **no** form of this command.

stcapp ccm-group *group-id*

no stcapp ccm-group *group-id*

Syntax Description

group-id	Cisco CallManager group number.

Command Default No Cisco CallManager group number is configured.

Command Modes Global configuration.,

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines The Cisco CallManager group identifier must have been configured for the service provider interface (SPI) using the **sccp ccm-group** *group-id* command.

Examples The following example configures the STCAPP to use Cisco CallManager group 2:

```
Router(config)# stcapp ccm-group 2
```

Related Commands

Command	Description
show stcapp device	Displays configuration information about SCCP Telephony Control Application (STCAPP) voice ports.
show stcapp statistics	Displays call statistics for SCCP Telephony Control Application (STCAPP) voice ports.
stcapp	Enables the SCCP Telephony Control Application (STCAPP).
stcapp timer	Enables SCCP Telephony Control Application (STCAPP) timer configuration.

stcapp feature access-code

To enable STC application feature access codes and enter their configuration mode, use the **stcapp feature access-code** command in global configuration mode. To disable the use of all STC application feature access codes, use the **no** form of this command.

stcapp feature access-code

no stcapp feature access-code

Syntax Description

This command has no arguments or keywords.

Command Default

All feature access codes are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the SCCP telephony control (STC) application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Although feature access prefixes and codes for analog FXS ports are configured on the Cisco VG 224, pickup groups and call-forwarding destinations are configured on Cisco CallManager or the Cisco CallManager Express system.

Note that all the STC feature access codes (FACs) have defaults. To return FACs under this configuration mode to their defaults, you must use the **no** form of the individual commands one at a time.

The **no** form of this command blocks the use of FACs on all analog ports.

Examples

The following example sets a FAC prefix of two pound signs (##) and a call-forward-all FAC of 2. After these values are configured, a phone user presses ##2 on the keypad to forward all calls for that extension.

```
Router(config)# stcapp feature access-code
Router(stcapp-fac)# prefix ##
Router(stcapp-fac)# call forward all 2
Router(stcapp-fac)# call forward cancel 3
Router(stcapp-fac)# pickup local 6
Router(stcapp-fac)# pickup group 5
Router(stcapp-fac)# pickup direct 4
Router(stcapp-fac)# exit
```

Related Commands

Command	Description
call forward all	Designates an STC application feature access code to activate the forwarding of all calls.
call forward cancel	Designates an STC application feature access code to cancel the forwarding of all calls.
pickup direct	Designates an STC application feature access code for directed call pickup.
pickup group	Designates an STC application feature access code for group call pickup from another group.
pickup local	Designates an STC application feature access code for group call pickup from the local group.
prefix	Designates a prefix to precede the dialing of an STC application feature access code.
show stcapp feature codes	Displays configured and default STC application feature access codes.

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback

no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application.

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp feature speed-dial

To enable STC application feature speed-dial codes and enter their configuration mode, use the **stcapp feature speed-dial** command in global configuration mode. To disable the use of all STC application feature speed-dial codes, use the **no** form of this command.

stcapp feature speed-dial

no stcapp feature speed-dial

Syntax Description This command has no arguments or keywords.

Command Default All feature speed-dial codes are disabled.

Command Modes Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines This command is used with the SCCP telephony control (STC) application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Although feature speed-dial (FSD) prefixes and codes for analog FXS ports are configured on the voice gateway that has the FXS ports, the actual numbers that are dialed using these codes are configured on Cisco CallManager or the Cisco CallManager Express system.

The **no** form of this command blocks the use of FSD codes on all analog ports.

Note that all the STC FSD codes have defaults. To return codes under this configuration mode to their defaults, you must use the **no** form of the individual commands one at a time.

Examples The following example sets an FSD prefix of three asterisks (***) and speed-dial codes from 2 to 7. After these values are configured, a phone user presses ***2 on the keypad to speed-dial the telephone number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ***
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# redial 9
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

```
Router# show stcapp feature codes
.
.
.
  stcapp feature speed-dial
    prefix ***
    redial ***9
    voicemail ***8
    speeddial1 ***2
    speeddial2 ***3
    speeddial3 ***4
    speeddial4 ***5
    speeddial5 ***6
    speeddial6 ***7
```

Related Commands

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show stcapp feature codes	Displays configured and default STC application feature codes.
speed dial	Designates a range of STC application feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

stcapp register capability

To specify modem capability for SCCP Telephony Control Application (STCAPP) devices, use the **stcapp register capability** command in global configuration mode. To disable modem capability, use the **no** form of this command.

stcapp register capability *voice-port* **[both | modem-passthrough | modem-relay]**

no stcapp register capability *voice-port*

Syntax Description

voice-port	Voice interface slot number 1 through 4
both	Specifies support for both modem-relay and modem pass-through.
modem-passthrough	Specifies support for modem pass-through.
modem-relay	Specifies support for V.150.1 modem relay.

Command Default

No voice port modem capability is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **stcapp register capability** *command to specify modem transport methods for STCAPP-controlled devices registering with Cisco Call-Manager. If this command is applied while the voice port is idle, the port automatically reregisters with the Cisco CallManager. If there is an active call on the voice port when this command is applied, the port does not reregister.* Although Cisco does not recommend the procedure, to force device reregistration you must either manually shut down the device using the **shutdown** command in voice-port configuration mode, or reset it from the Cisco CallManager.

Use the voice service configuration command **modem passthrough** to globally enable modem pass-through capability, thereby providing fallback to voice band data (modem pass-through) when the voice gateway communicates with a Secure Telephone Unit (STU) or nonmodem-relay capable gateway.

Examples

The following example configures the device connected to voice port 1/1/0 to support both modem capabilities:

```
Router(config)# stcapp register capability 1/1/0 both
```

Related Commands

Command	Description
modem passthrough	Globally enables modem pass-through over VoIP.
show stcapp device voice-port	Displays configuration information for STCAPP devices.
shutdown	Disables voice ports on the VIC.

stcapp security mode

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the security mode to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security mode** command in global configuration mode. To disable security for the endpoint, use the no form of this command.

stcapp security mode [**authenticated** | **encrypted** | **none**]

no stcapp security

Syntax Description

mode	Sets the global security mode for all STCAPP endpoints.
authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME through the secure TLS connection on TCP port 2443.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
none	Sets the security mode to none (Default).

Command Default

Security is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode** and **stcapp security trustpoint** commands to enable security for the STCAPP end point. The **stcapp security trustpoint** command must be configured for the STCAPP service to start.

SCCP signaling security mode can be set for each dial peer using the **security mode** command in dial peer configuration mode. If you use both the **stcapp security mode** and the **security mode** commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
security mode	Sets the security mode for a specific dial peer using STCAPP services in a secure Cisco Unified CME network.
stcapp	Enables the STCAPP.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.
stcapp security trustpoint	Enables security for STCAPP endpoints and specifies the trustpoint for setting up the TLS connection.

stcapp security trustpoint

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the trustpoint to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security** command in global configuration mode. To disable security for the endpoint and delete all identity information and certificates associated with the trustpoint, use the no form of this command.

stcapp security trustpoint *line*

no stcapp security

Syntax Description

trustpoint	Security trustpoint label for all STCAPP endpoints.
line	Text description that identifies the trustpoint.

Command Default

Security is not enabled and no trustpoint is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode** and **stcapp security trustpoint** commands to enable security for the STCAPP endpoint. The **stcapp security trustpoint** command must be configured for the STCAPP service to start. The trustpoint configured by this command contains the device certificate and must match the trustpoint configured on the router using the **crypto pki trustpoint** command. All analog phones use the same certificate. Cisco Unified Communications Manager Express does not require a different certificate for each phone.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.

Command	Description
stcapp	Enables the STCAPP.
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

stcapp supplementary-services

To enter supplementary-service configuration mode for configuring STC application supplementary-service features on an FXS port, use the **stcapp supplementary-services** command in global configuration mode. To remove the configuration, use the **no** form of this command.

stcapp supplementary-services

no stcapp supplementary-services

Syntax Description

This command has no arguments or keywords.

Command Default

No configuration for STC application supplementary-service features exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enters the supplementary-service configuration mode for configuring STC application supplementary-service features for analog FXS ports on a Cisco IOS voice gateway, such as a Cisco integrated services router (ISR) or Cisco VG224 Analog Phone Gateway.

Examples

The following example shows how to enable the Hold/Resume STC application supplementary-service feature for analog phones connected to port 2/0 on a Cisco VG224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
port (supplementary-service)	Specifies analog FXS port on which STC application supplementary-service features are to be supported.

stcapp timer

To enable SCCP Telephony Control Application (STCAPP) timer configuration, use the **stcapp timer** command in global configuration mode. To disable STCAPP timer configuration, use the **no** form of this command.

stcapp timer roh *seconds*

no stcapp timer

Syntax Description

roh	Receiver off hook (ROH) tone timeout.
seconds	Duration, in seconds, that the receiver off-key tone is played. Range is 0 to 120 seconds.

Command Default

seconds: 45 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure the STCAPP ROH timer for the maximum time that ROH tone is played. ROH tone signals a subscriber that the phone remains off hook when there is no active call.

Examples

The following example configures the receiver off hook timer for 30 seconds:

```
Router(config)# stcapp timer roh 30
```

Related Commands

Command	Description
show call application voice stcapp	Displays information about the STCAPP.
stcapp	Enables the STCAPP.

stun

To enter STUN configuration mode for configuring firewall traversal parameters, use the **stun** command in voice-service voip configuration mode. To remove stun parameters, use the **no** form of this command.

stun

no stun

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Voice-service voip configuration (config-voi-serv).

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines Use this command to enter the configuration mode to configure firewall traversal parameters for VoIP communications.

Examples The following example shows how to enter STUN configuration mode.

```
Router(config)#voice service voip
Router(config-voi-serv)#stun
```

Related Commands

Command	Description
stun flowdata agent-id	Configures the agent ID.
stun flowdata keepalive	Configures the keepalive interval.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun usage firewall-traversal flowdata	Enables firewall traversal using stun.
voice-class stun-usage	Enables firewall traversal for VoIP communications.

stun flowdata agent-id

To configure the stun flowdata agent ID, use the **stun flowdata agent-id** command in STUN configuration mode. To return to the default value for agent ID, use the **no** form of this command.

stun flowdata agent-id *tag* [*boot-count*]

no stun flowdata agent-id *tag* [*boot-count*]

Syntax Description

tag	Unique identifier in the range 0 to 255. Default is -1.
boot-count	(Optional) Value of boot-count. Range is 0 to 65535. Default is zero.

Command Default No firewall traversal is performed.

Command Modes STUN configuration (conf-serv-stun).

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines Use the **stun flowdata agent-id** command to configure the agent id and the boot count to configure call control agents which authorize the flow of traffic.

Configuring the boot-count keyword helps to prevent anti-replay attacks after the router is reloaded. If you do not configure a value for boot count, the boot-count is initialized to 0 by default. After it is initialized, it is incremented by one automatically upon each reboot and the value saved back to NVRAM. The value of boot count is reflected in **show running** configuration command.

Examples The following example shows how the **stun flowdata agent-id** command is used at the router prompt.

```
Router#enable
Router#configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata agent-id 35 100
```

Related Commands

Command	Description
stun flowdata keepalive	Configures the keepalive interval.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.

stun flowdata catlife

To configure the lifetime of the CAT, use the **stun flowdata catlife** command in STUN configuration mode. To return to the default catlife value, use the **no** form of this command.

stun flowdata catlife *liftetime* **keepalive** *interval*

no stun flowdata catlife *liftetime* **keepalive** *interval*

Syntax Description

liftetime	Lifetime of the CAT in seconds. The default value is 1270 (21 min 10 sec).
interval	Keepalive interval time in seconds. Range is 10 to 30. Default is 10.

Command Default

The default keepalive value is 10 seconds.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **stun flowdata catlife** command to configure call control agents which authorize the flow of traffic.

Examples

The following example shows how the **stun flowdata catlife** command is used at the router prompt.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata catlife 150 keepalive 30
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun flowdata agent-id	Configures the agent ID.

stun flowdata keepalive

Note Effective with Cisco IOS Release 15.0(1)M, the **stun flowdata keepalive** command is replaced by the command **stun flowdata catlife**.

To configure the keepalive interval, use the **stun flowdata keepalive** command in STUN configuration mode. To return to the default keepalive value, use the **no** form of this command.

stunflowdata keepalive *seconds*

no stunflowdata keepalive *seconds*

Syntax Description

seconds	Keepalive interval in seconds. Range is 1 to 65535. Default is 10.

.

Command Default The default keepalive value is 10 seconds.

Command Modes STUN configuration (conf-serv-stun).

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.0(1)M	This command was replaced. The call application **stun flowdata keepalive** command was replaced by the commands **stun flowdata catlife**. The **stun flowdata keepalive** command is hidden and depreciated in Cisco IOS Release 15.0(1)M.

Usage Guidelines You can use the **stun flowdata keepalive** command to decide how often to send keepalives. Keepalives are application mechanisms for maintaining alive the firewall traversal mappings associated with firewalls.

TRP works with a Call Agent which supports firewall traversal. In this mode, the Call Agent sends a request to TRP to open the pinhole. The request contains local, remote IP /Port, token, and other Cisco-flow data parameters.

TRP sends a STUN indication message to the firewall with Cisco-flow data, after processing the request. The message contains the STUN header, STUN username, and Cisco-flow data. The firewall validates the token in Cisco-flow data after receiving the STUN packet, and opens the pinhole if validation is successful.

Keepalives in STUN flow between the UDP peers to ensure that the firewall keeps the pinholes open.

This command is hidden and depreciated in Cisco IOS Release 15.0(1)M release because the keepalive interval is configured along with stun flowdata catlife command. When this command is configured or present in start-up configuration during reload, the following command will be nvgen'ed and displayed in **show run** command.

In addition, the following message will be printed during the configuration/reload:

```
Deprecated command. Setting catlife=1270 sec and keepalive=30 sec.
Use the following command to configure non-default values:
stun flowdata catlife <lifetime> keepalive <interval>
```

Examples

The following example shows how to change the **stun flowdata keepalive interval** from the default value (10) to 5 seconds.

```
Router(config)# voice service voip
Router(config-voi-serv)#stun
Router(config-serv-stun)#stun flowdata agent-id 35
Router(config-serv-stun)#stun flowdata shared-secret 123abc123abc
Router(config-serv-stun)#stun flowdata keepalive 5
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun flowdata agent-id	Configures the agent ID.

stun flowdata shared-secret

To configure a secret shared on a call control agent, use the **stun flowdata shared-secret** command in STUN configuration mode. To return the shared secret to the default value, use the **no** form of this command.

stun flowdata shared-secret [*tag*] *string*

no stun flowdata shared-secret [*tag*] *string*

Syntax Description

tag	(Optional) 0—Defines the password in plaintext and will encrypt the password. (Optional) 7— Defines the password in encrypted form and will validate the (encrypted) password before accepting it.
string	12 to 80 ASCII characters. Default is an empty string.

Command Default

The default value of this command sets the shared secret to an empty string. No firewall traversal is performed when the shared-secret has the default value.

Command Modes

STUN configuration (conf-serv-stun).

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.0(1)M	This command was modified. The encryption values zero and seven was added to this command.

Usage Guidelines

A shared secret on a call control agent is a string that is used between a call control agent and the firewall for authentication purposes. The shared secret value on the call control agent and the firewall must be the same. This is a string of 12 to 80 characters. The **no** form of this command will remove the previously configured shared-secret if any. The default form of this command will set the shared-secret to NULL. The password can be encrypted and validated before it is accepted. Firewall traversal is not performed when the shared-secret is set to default.

Examples

The following example shows how the **stun flowdata shared-secret** command is used.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(config-serv-stun)#stun flowdata shared-secret 123cisco123cisco
```

Related Commands

Command	Description
stun	Enters st un configuration mode.
stun flowdata agent-id	Configures the agent ID.
stun flowdata catlife	Configures the lifetime of the CAT.

stun usage firewall-traversal flowdata

To enable firewall traversal using stun, use the **stun usage firewall-traversal flowdata** command in voice class stun-usage configuration mode. To disable firewall traversal with stun, use the **no** form of this command.

stun usage firewall-traversal flowdata

no stun usage firewall-traversal flowdata

Syntax Description

This command has no arguments or keywords.

Command Default

Firewall traversal using STUN is not enabled.

Command Modes

Voice-class configuration (config-class).

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows how to enable firewall traversal using STUN:

```
Router(config)#voice class stun-usage 10
Router(config-class)#stun usage firewall-traversal flowdata
```

Related Commands

Command	Description
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.

subaddress

To configure a subaddress for a POTS port, use the **subaddress** command in dial peer voice configuration mode. To disable the subaddress, use the **no** form of this command.

subaddress *number*

no subaddress *number*

Syntax Description

number	Actual subaddress of the POTS port.

Command Default No subaddress is available for a POTS port.

Command Modes Dial peer voice configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines You can use this command for any dial-peer voice POTS port. You can configure only one subaddress for each of the POTS ports. The latest entered subaddress on the dial-peer voice port is stored. To check the status of the subaddress configuration, use the **show running-config** command.

Examples The following examples show that a subaddress of 20 has been set for POTS port 1 and that a subaddress of 10 has been set for POTS port 2:

```
dial-peer voice 1 pots
 destination-pattern 5555555
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 1111111 ring 3
 caller-number 2222222 ring 1
 caller-number 3333333 ring 1
 subaddress 20

dial-peer voice 2 pots
 destination-pattern 4444444
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 6666666 ring 2
 caller-number 7777777 ring 3
 subaddress 10
```

subcell-mux

To enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing on a Cisco router, use the **subcell-mux** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

subcell-mux *time*

no subcell-mux *time*

Syntax Description

time	Timer value, in milliseconds. Range is from 5 to 1000 (1 second). Default is 10. The *time* argument is implemented for Cisco 3600 routers.

Command Default

10 ms
Subcell multiplexing is off

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)XB	The *time* argument was implemented on the Cisco 3660.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing when the Cisco router interoperates with other equipment that uses subcell multiplexing.

Examples

The following example sets AAL2 CPS subcell multiplexing to 15 ms:

```
Router(conf-voi-serv-sess)# subcell-mux 15
```

Related Commands

Command	Description
voice-service	Specifies the voice encapsulation type and enters voice-service configuration mode.

subscription asnl session history

To specify how long to keep Application Subscribe/Notify Layer (ASNL) subscription history records and how many history records to keep in memory, use the **subscription asnl session history** command in global configuration mode. To reset to the default, use the no form of this command.

subscription asnl session history {**count** *number* | **duration** *minutes*}

no subscription asnl session history {**count** | **duration**}

Syntax Description

count *number*	Number of records to retain in a session history.
duration *minutes*	Duration, in minutes, for which to keep the record.

Command Default

Default duration is 10 minutes. Default number of records is 50.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The ASNL layer maintains subscription information. Active subscriptions are retained in the active subscription table in system memory. When subscriptions are terminated, they are moved to the subscription table in system memory.

This command controls the ASNL history table. Use this command to specify how many minutes the history record is retained after the subscription is removed, and to specify how many records are retained at any given time.

Examples

The following example specifies that a total of 100 records are to be kept in the RTSP client history:

```
subscription asnl session history count 100
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

subscription maximum

To specify the maximum number of outstanding subscriptions to be accepted or originated by a gateway, use the **subscription maximum** command in voice service voip sip configuration mode. To remove the maximum number of subscriptions specified, use the **no** form of this command.

subscription maximum {**accept** | **originate**} *number*

no subscription maximum {**accept** | **originate**}

Syntax Description

accept	Subscriptions accepted by the gateway.
originate	Subscriptions originated by the gateway.
number	Maximum number of outstanding subscriptions to be accepted or originated by the gateway.

Command Default

The default number of subscriptions is equal to twice the number of dial-peers configured on the platform.

Command Modes

Voice service voip sip configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to configure the maximum number of concurrent SIP subscriptions, up to twice the number of dial-peers configured.

Examples

The following example configures subscription maximums:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# subscription maximum originate 10
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
retry timer	Configures the retry interval for resending SIP messages.
show subscription	Displays active SIP subscriptions.

supervisory answer dualtone

To enable answer supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory answer dualtone command in** voice-port configuration mode. To disable answer supervision on a voice port, use the **no** form of this command.

supervisory answer dualtone [**sensitivity** {**high** | **medium** | **low**}]

no supervisory answer dualtone

Syntax Description

sensitivity	(Optional) Specific detection sensitivity for answer supervision.
high	Increased level of detection sensitivity.
medium	Default level of detection sensitivity.
low	Decreased level of detection sensitivity.

Command Default

Answer supervision is not enabled on voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(2)T	This command was introduced on the following platforms: Cisco 1750, Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

This command configures the FXO voice port to detect voice, fax, and modem traffic when calls are answered. If answer supervision is enabled, calls are not recorded as connected until answer supervision is triggered.

This command enables a ring-no-answer timeout that drops calls after a specified period of ringback. The period of ringback can be configured using the **timeouts ringing** command.

This command automatically enables disconnect supervision in the preconnect mode on the voice port if disconnect supervision is not already enabled with the **supervisory disconnect dualtone** command.

This command is applicable to analog FXO voice ports with loop-start signaling.

If false answering is detected, decrease the **sensitivity** setting. If answering detection is failing, increase the **sensitivity** setting.

Examples

The following example enables answer supervision on voice port 0/1/1:

```
voice-port 0/1/1
 supervisory answer dualtone
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts ringing	Specifies the time that the calling voice port allows ringing to continue if a call is not answered.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory custom-cptone

To associate a class of custom call-progress tones with a voice port, use the **supervisory custom-cptone command in** voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory custom-cptone *cptone-name*

no supervisory custom-cptone

Syntax Description

cptone-name	Descriptive identifier of the class of custom call-progress tones to be detected by a voice port. This name must match the *cptone-name* of a class of tones defined by the **voice class custom-cptone** command.

Command Default

U.S. standard call-progress tones are associated with a voice port.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a class of custom call-progress tones, defined by the **voice class custom-cptone** command, with a voice port.

You can associate the same custom call-progress tones to multiple voice ports.

You can associate only one class of custom call-progress tones with a voice port. If you associate a second class of custom call-progress tones with a voice port, the second class of custom tones replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of custom call-progress tones named country-x with voice ports 1/4 and 1/5:

```
voice-port 1/4
 supervisory custom-cptone country-x
 exit
voice-port 1/5
 supervisory custom-cptone country-x
 exit
```

Related Commands

Command	Description
dualtone	Defines a call-progress tone to be detected.
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

supervisory disconnect

To enable a supervisory disconnect signal on Foreign Exchange Office (FXO) ports, use the **supervisory disconnect** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect

no supervisory disconnect

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines This command indicates whether supervisory disconnect signaling is available on the FXO port. Supervisory disconnect signaling is a power denial from the switch lasting at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call.

You should configure no supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch.

Note If there is no disconnect supervision on the voice port, the interface could be left active if the caller abandons the call before the far end answers. After the router collects the dialed digits but before the called party answers, the router starts a tone detector. Within this time window, the tone detector listens for signals (such as a fast busy signal) that occur if the originating caller hangs up. If this occurs, the router interprets those tones as a disconnect indication and closes the window.

Examples The following example configures supervisory disconnect on a voice port:

```
voice-port 2/1/0
 supervisory disconnect
```

supervisory disconnect anytone

To configure a Foreign Exchange Office (FXO) voice port to go on-hook if the router detects any tone from a PBX or the PSTN before an outgoing call is answered, use the **supervisory disconnect anytone command in** voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect anytone

no supervisory disconnect anytone

Syntax Description

This command has no arguments or keywords.

Command Default

The supervisory disconnect function is not enabled on voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

Use this command to provide disconnect if the PBX or PSTN does not provide a supervisory tone. Examples of tones that trigger a disconnect include busy tone, fast busy tone, and dial tone.

This command is enabled only during call setup (before the call is answered).

You must enable echo cancellation; otherwise, ringback tone from the router can trigger a disconnect.

This command replaces the **no supervisory disconnect signal** command. If you enter this command, the supervisory disconnect anytone feature is enabled, and the message `supervisory disconnect anytone` is displayed when **show** commands are entered.

If you enter either the **supervisory disconnect anytone** command or the **no supervisory disconnect signal** command, answer supervision is automatically disabled.

Examples

The following example configures voice ports 1/4 and 1/5 to go on-hook if any tone from the PBX or PSTN is detected before the call is answered:

```
voice-port 1/4
 supervisory disconnect anytone
 exit
voice-port 1/5
 supervisory disconnect anytone
 exit
```

The following example disables the disconnect function on voice port 1/5:

```
voice-port 1/5
 no supervisory disconnect anytone
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.

supervisory disconnect dualtone

To enable disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory disconnect dualtone command in** voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**}

no supervisory disconnect dualtone

Syntax Description

mid-call	Disconnect supervision operates throughout the duration of the call.
pre-connect	Disconnect supervision operates during call setup and stops when the called telephone goes off-hook.

Command Default

Disconnect supervision is not enabled on voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command configures an FXO voice port to disconnect calls when the router detects call-progress tones from a PBX or the PSTN. Disconnection occurs after the wait-release time specified on the voice port.

Disconnect supervision is automatically enabled in the preconnect mode on the voice port if the **supervisory answer dualtone** command is entered.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples

The following example specifies tone detection during the entire call duration:

```
voice-port 1/5
 supervisory disconnect dualtone mid-call
 exit
```

The following example specifies tone detection only during call setup:

```
voice-port 0/1/1
 supervisory disconnect dualtone pre-connect
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.
timeouts wait-release	Specifies the timeout value for releasing a voice port when an outgoing call is not answered.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory disconnect dualtone voice-class

To assign a previously configured voice class for Foreign Exchange Office (FXO) supervisory disconnect tone to a voice port, use the **supervisory disconnect dualtone voice-class** command in voice port configuration mode. To remove a voice class from a voice-port, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**} **voice-class** *tag*

no supervisory disconnect dualtone voice-class *tag*

Syntax Description

mid-call	Tone detection operates throughout the duration of a call.
pre-connect	Tone detection operates during call setup and stops when the called telephone goes off-hook.
tag	Unique identification number assigned to one voice class. The tag number maps to the tag number assigned using the **voice class dualtone** global configuration command. Range is from 1 to 10000.

Command Default No voice class is assigned to a voice port.

Command Modes Voice-port configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines You can apply an FXO supervisory disconnect tone voice class to multiple voice ports. You can assign only one FXO supervisory disconnect tone voice class to a voice port. If a second voice class is assigned to a voice port, the second voice class replaces the one previously assigned. You cannot assign separate FXO supervisory disconnect tone commands directly to the voice port.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples The following example assigns voice class 70 to FXO voice port 0/1/1 and specifies tone detection during the entire call duration:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone mid-call voice-class 70
```

The following example assigns voice class 80 to FXO voice port 0/1/1 and specifies tone detection only during call setup:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone pre-connect voice-class 80
```

Related Commands

Command	Description
channel-group	Defines the time slots of each T1 or E1 circuit.
mode	Sets the mode of the T1/E1 controller and enters specific configuration commands for each mode type in VoATM.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

supervisory disconnect lcfo

To enable a supervisory disconnect signal on an FXS port, use the **supervisory disconnect lcfo** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect lcfo

no supervisory disconnect lcfo

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)YD	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(2)T	Support was added for SCCP Telephony Control Application (STCAPP) analog voice ports.

Usage Guidelines

This command enables a disconnect indication by triggering a power denial using a loop current feed open (LCFO) signal on FXS ports with loop-start signaling. Third-party devices, such as an interactive voice response (IVR) system, can detect a disconnect and clear the call when it receives the power denial signal. To disable the power denial during the disconnect stage, use the **no supervisory disconnect lcfo** command. The duration of the power denial is set with the **timeouts power-denial** command.

Examples

The following example disables the power denial indication on voice port 2/0:

```
voice-port 2/0
 no supervisory disconnect lcfo
```

Related Commands

Command	Description
timeouts power-denial	Sets the duration of the power denial timeout for a specified FXS voice port.

supervisory dualtone-detect-params

To associate a class of modified tone-detection tolerance limits with a voice port, use the **supervisory dualtone-detect-params command in** voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory dualtone-detect-params *tag*

no supervisory dualtone-detect-params

Syntax Description

tag	Tag number of the set of modified tone-detection tolerance limits to be associated with the voice port. The tag number must match the tag number of a voice class configured by the **voice class dualtone-detect-params** command. Range is from 1 to 10000.

Command Default

The default tone-detection tolerance limits are associated with voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a specific set of modified tone-detection tolerance limits, defined by the **voice class dualtone-detect-params** command, with a voice port.

You can associate the same class of modified tone-detection tolerance limits to multiple voice ports.

You can associate only one class of modified tone-detection tolerance limits to a voice port. If you associate a second class of modified tone-detection tolerance limits with a voice port, the second class replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of modified tone-detection tolerance limits that has tag 70 with voice ports 1/5 and 1/6.

```
voice-port 1/5
 supervisory dualtone-detect-params 70
 exit
voice-port 1/6
 supervisory dualtone-detect-params 70
 exit
```

The following example restores the default tone-detection parameters to voice port 1/5.

```
voice-port 1/5
 no supervisory dualtone-detect-params
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class dualtone-detect-params	Creates a voice class for call-progress tone-detection tolerance parameters.

supervisory sit us

To provide detection of eight standard U.S. special information tones (SITs) and certain nonstandard tones (including the AT&T SIT), and to report the detected tone with a preassigned disconnect cause code for disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory sit us** command in voice-port configuration mode. To turn off the detection and disconnect activity, use the **no** form of this command.

supervisory sit us [**all-tones**] [**tone-selector** *value*] [**immediate-release**]

no supervisory sit us

Syntax Description

all-tones	(Optional) Disconnects the call when a SIT or a nonstandard tone is detected.
tone-selector	(Optional) Defines a specific response for call-disconnect when a standard SIT or a nonstandard tone is detected on the incoming or outgoing call.
value	Acceptable values are 0, 1, 2, or 3: • 0—Detection of a standard SIT drops the call, but an AT&T SIT or a nonstandard tone does not cause a disconnect. • 1—Detection of either a standard SIT or nonstandard tone drops the call, but the AT&T SIT does not cause a disconnect. • 2—Detection of a standard SIT or an AT&T SIT results in a call disconnect, but any other nonstandard tone does not cause a disconnect. • 3—Detection of a standard SIT, AT&T SIT, or another nonstandard tone results in a disconnect.
immediate-release	(Optional) Disconnects the call immediately when a SIT is detected on the incoming or outgoing call. Nonstandard tones are ignored.

Command Default

No detection or disconnect occurs for the eight standard U.S. SITs, nonstandard tones, or the AT&T SIT on the FXO voice port for incoming and outgoing calls.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
12.4(24)T	The **all-tones** and **tone-selector** keywords and the *value* argument were added.

Usage Guidelines

This command configures an FXO voice port to detect and disconnect calls when the router detects call-progress tones from a PBX or the PSTN.

Prior to Cisco IOS Release 12.4(24)T, this command specifically detected eight standard U.S. SITs, but not nonstandard tones or the AT&T SIT. Beginning in Cisco IOS Release 12.4(24)T, the **tone-selector** *value* option can be configured to detect nonstandard tones played by the service provider when the called number is invalid.

Disconnection occurs after the wait-release time specified on the voice port. Calls are disconnected immediately after a SIT is detected from the PSTN when the **immediate-release** keyword is configured. To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release** command on the voice port.

The SIT reporting complies with standard Q.850 messages in order for fax servers to uniquely identify each condition. This capability is supported for analog FXO trunk and T1/E1 channel-associated signaling (CAS) FXO loop-start.

Note The SIT detection and reporting feature enabled by the **supervisory sit us** command is supported on c5510 and LSI digital signal processors (DSPs). No other DSPs support this feature.

Table 240 identifies eight standard U.S. SITs and their associated disconnect cause codes.

Note These eight tones are referred to as standard tones based on the tone frequencies and durations shown in the table. These tones are defined in the Telcordia Technologies specification GR-1162-CORE (which is specific to North America). There are other nonstandard SITs that can occur. The AT&T SIT is one of the more common examples of the other variations. The nonstandard SITs can have durations and frequencies comparable to the nominal values for the eight tone segments shown in Table 240 or the nonstandard SITs can deviate significantly from these nominal values. The **supervisory sit us** command has been modified in Cisco IOS Release 12.4(24)T to provide flexibility in handling these variations.

Table 240 Eight U.S. SITs and Associated Disconnect Cause Codes

Name	First Tone (Hz)	ms	Second Tone (Hz)	ms	Third Tone (Hz)	ms	Disconnect Cause Code
IC	913.8	274	1370.6	274	1776.7	380	8
VC	985.2	380	1370.6	274	1776.7	380	1
RO	985.2	274	1370.6	380	1776.7	380	86
RO	913.8	274	1428.5	380	1776.7	380	86
NC	913.8	380	1370.6	380	1776.7	380	34
NC	985.2	380	1428.5	380	1776.7	380	34
#1	913.8	380	1428.5	274	1776.7	274	21
#2	985.2	274	1428.5	274	1776.7	380	21

Examples

The following example shows how to enable SIT detection for the eight standard U.S. tones and provide for immediate disconnect on the voice port:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us immediate-release
```

The following example shows how to enable SIT detection for all eight standard U.S. tones and configure the delay timeout for 10 seconds:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us
Router(config-voiceport)# timeouts wait-release 10
```

The following example shows how to enable detection for a standard SIT or the AT&T SIT and to provide for immediate disconnect on the voice port (in this case, a nonstandard SIT does not cause a disconnect):

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us tone-selector 2 immediate-release
```

Related Commands

Command	Description
timeouts wait-release	Configures the delay timeout before the system starts the process for releasing voice ports.

supplementary-service h225-notify cid-update (dial peer)

To enable individual dial peers to send H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in dial peer configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update

no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies that an individual dial peer should provide caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode to specify this capability globally.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
supplementary-service h225-notify cid-update (voice-service)	Globally enables the sending of H.225 messages with caller-ID updates.

supplementary-service h225-notify cid-update (voice-service)

To globally enable the sending of H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update

no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command globally provides caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in dial peer configuration mode to specify this capability for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
supplementary-service h225-notify cid-update (dial peer)	Enables the sending of H.225 messages with caller-ID updates for individual dial peers.
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.2 (dial peer)

To enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.2** command in dial peer configuration mode. To disable H.450.2 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.2

no supplementary-service h450.2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies the use of the H.450.2 standard protocol for call transfers across a VoIP network for the calls handled by an individual dial peer. Use the **supplementary-service h450.2** command in voice-service configuration mode to specify H.450.2 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.2 services for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# no supplementary-service h450.2
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
supplementary-service h450.2 (voice-service)	Globally enables H.450.2 capabilities for call transfers.

supplementary-service h450.2 (voice-service)

To globally enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.2** command in voice-service configuration mode. To disable H.450.2 capabilities globally, use the **no** form of this command.

supplementary-service h450.2

no supplementary-service h450.2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.2 standard protocol for call transfers for all calls across a VoIP network. Use the **no supplementary-service h450.2** command in dial peer configuration mode to disable H.450.2 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.2 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.2
Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.2 (dial peer)	Enables H.450.2 call transfer capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.3 (dial peer)

To enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network for an individual dial peer, use the **supplementary-service h450.3** command in dial peer configuration mode. To disable H.450.3 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.3

no supplementary-service h450.3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.3 standard protocol for call forwarding for calls handled by an individual dial peer. Use the **supplementary-service h450.3** command in voice-service configuration mode to specify H.450.3 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.3 capabilities for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# no supplementary-service h450.3
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.

supplementary-service h450.3 (voice-service)

To globally enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network, use the **supplementary-service h450.3** command in voice-service configuration mode. To disable H.450.3 capabilities globally, use the **no** form of this command.

supplementary-service h450.3

no supplementary-service h450.3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.3 standard protocol for call forwarding across a VoIP network. Use the **no supplementary-service h450.3** command in dial peer configuration mode to disable H.450.3 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.3 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.3
Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.3 (dial peer)	Enables H.450.3 call forwarding capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.7

To globally enable H.450.7 supplementary services capabilities exchange for message-waiting indication (MWI) across a VoIP network, use the **supplementary-service h450.7** command in voice-service or dial peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service h450.7

no supplementary-service h450.7

Syntax Description

There are no keywords or arguments.

Command Default

H.450.7 supplementary services are disabled.

Command Modes

Voice-service configuration
Dial peer configuration

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use this command when you are implementing QSIG supplementary service features that use the H.450.7 standard.

Use this command in voice-service configuration mode to affect all dial peers globally. Use this command in dial peer configuration mode to affect an individual dial peer:

If the **supplementary-service h450.7** command is not in use, the services are globally disabled by default.

If the **supplementary-service h450.7** command is not in use in voice-service configuration mode, you can use this command in dial peer configuration mode to enable the services on individual dial peers.

If the **supplementary-service h450.7** command is in use in voice-service configuration mode, the services are globally enabled and you cannot disable the services on individual dial peers.

Examples

The following example shows how to globally enable H.450.7 supplemental services:

```
voice service voip
 supplementary-service h450.7
```

The following example shows how to enable H.450.7 supplemental services on dial peer 256:

```
dial-peer voice 256 voip
 supplementary-service h450.7
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.12 (dial peer)

To enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.12** command in dial peer configuration mode. To disable H.450.12 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.12

no supplementary-service h450.12

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.12 standard protocol for call transfers across a VoIP network for calls handled by an individual dial peer. Use the **supplementary-service h450.12** command in voice-service configuration mode to specify H.450.12 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Examples

The following example enables H.450.12 capabilities on dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# supplementary-service h450.12
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
supplementary-service h450.12 (voice-service)	Globally enables H.450.12 capabilities.

supplementary-service h450.12 (voice-service)

To globally enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.12** command in voice-service configuration mode. To disable H.450.12 capabilities globally, use the **no** form of this command.

supplementary-service h450.12 [**advertise-only**]

no supplementary-service h450.12 [**advertise-only**]

Syntax Description

advertise-only	(Optional) Advertises H.450 capabilities to the remote end but does not require H.450.12 responses.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The H.450.12 standard provides a means to advertise and discover H.450.2 call transfer and H.450.3 call forwarding capabilities in voice gateway endpoints on a call-by-call basis. When H.450.12 is enabled, use of H.450.2 and H.450.3 standards is disabled for call transfers and call forwards unless a positive H.450.12 indication is received from all the other VoIP endpoints involved in the call. If positive H.450.12 indications are received, the router uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding. If a positive H.450.12 indication is not received, the router uses the alternative method that you have configured for call transfers and forwards, which, for Cisco CallManager Express (Cisco CME) 3.1 systems, may be either hairpin call routing or an H.450 tandem gateway. This command is useful when you have a mixed network with some endpoints that support H.450.2 and H.450.3 standards and other endpoints that do not support those standards.

This command specifies the global use of the H.450.12 standard protocol for all calls across a VoIP network. Use the **supplementary-service h450.12** command in dial peer configuration mode to specify H.450.12 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Use the **advertise-only** keyword on a Cisco CME 3.1 system when you have only Cisco CME 3.0 systems in your network in addition to Cisco CME 3.1 systems. Cisco CME 3.0 systems can use H.450.2 and H.450.3 standards, but are unable to respond to H.450.12 queries. The **advertise-only** keyword enables a Cisco CME 3.1 system to bypass the requirement that a system respond to an H.450.12 query in order to use H.450.2 and H.450.3 standards for transferring and forwarding calls.

Examples

The following example enables H.450.12 capabilities at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12
Router(config-voi-serv)# exit
```

The following example enables H.450.12 capabilities at a global level in advertise-only mode on a Cisco CME 3.1 system to enable call transfers using the H.450.2 standard and call forwards using the H.450.3 standard with Cisco CME 3.0 systems in the network.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12 advertise-only
Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.12 (dial peer)	Enables H.450.12 capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service media-renegotiate

To globally enable midcall media renegotiation for supplementary services, use the **supplementary-service media-renegotiate** command in voice-service configuration mode. To disable midcall media renegotiation for supplementary services, use the **no** form of this command.

supplementary-service media-renegotiate

no supplementary-service media-renegotiate

Syntax Description This command has no arguments or keywords.

Command Default Midcall media renegotiation for supplementary services is disabled.

Command Modes Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines This command enables midcall media renegotiation, or key renegotiation, for all calls across a VoIP network. To implement media encryption, the two endpoints controlled by Cisco Unified Communications Manager Express (Cisco Unified CME) need to exchange keys that they will use to encrypt and decrypt packets. Midcall key renegotiation is required to support interoperation and supplementary services among multiple VoIP suites in a secure media environment using Secure Real-Time Transport Protocol (SRTP).

Note The video part of a video stream will not play if the **supplementary-service media-renegotiate** command is configured in voice-service configuration mode.

Examples The following example enables midcall media renegotiation for supplementary services at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service media-renegotiate
Router(config-voi-serv)# exit
```

supplementary-service qsig call-forward

To specify that calls are using QSIG and require supplementary services for call forwarding, use the **supplementary-service qsig call-forward** command in voice-service or dial peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service qsig call-forward

no supplementary-service qsig call-forward

Syntax Description

This command has no keywords or arguments.

Command Default

The functionality is disabled.

Command Modes

Voice-service configuration
Dial peer configuration

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command provides QSIG call-forwarding supplementary services (ISO 13873) when necessary to forward calls to another number.

Use this command in voice-service configuration mode, which is enabled by the **voice service pots** command, to affect all POTS dial peers globally. Use this command in dial peer configuration mode, which is enabled by the **dial-peer voice** command, to affect a single POTS dial peer.

If you are not using the **supplementary-service qsig call-forward** command, the services are globally disabled by default.

If you are not using the **supplementary-service qsig call-forward** command in voice-service configuration mode, you can use this command in dial peer configuration mode to enable the services on individual POTS dial peers.

If you are using the **supplementary-service qsig call-forward** command in voice-service configuration mode, this feature is globally enabled and you cannot disable the services on individual POTS dial peers.

Examples

The following example shows how to enable QSIG call-forwarding treatment for all POTS calls:

```
Router(config)# voice service pots
Router(conf-voi-serv)# supplementary-service qsig call-forward
```

The following example shows how to enable QSIG call-forwarding treatment for calls on POTS dial-peer 23:

```
Router(config)# dial-peer voice 23 pots
Router(config-dial-peer)# supplementary-service qsig call-forward
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode.
voice service voip	Enters voice-service configuration mode.

supplementary-service sip

To enable SIP supplementary service capabilities for call forwarding and call transfers across a SIP network, use the **supplementary-service sip** command in dial-peer or voice service voip configuration mode. To disable supplementary service capabilities, use the **no** form of this command.

supplementary-service sip {**moved-temporarily** | **refer**}

no supplementary-service sip {**moved-temporarily** | **refer**}

Syntax Description

moved-temporarily	SIP redirect response for call forwarding.
refer	SIP REFER message for call transfers.

Command Default

SIP supplementary service capabilities are enabled globally.

Command Modes

Dial-peer configuration (config-dial-peer)
Voice-service voip configuration (conf-voi-serv)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command allows you to disable a supplementary service feature (call forwarding or call transfer) if the destination gateway does not support the supplementary service. You can disable the feature either globally or for a specific SIP trunk (dial peer) by using the **no** form of this command.

The **no supplementary-service sip moved-temporarily** command prevents the router from sending a redirect response to the destination for call forwarding. The **no supplementary-service sip refer** command prevents the router from forwarding a REFER message to the destination for call transfers. The router instead attempts to initiate a hairpin call to the new target.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

This command is supported for calls between SIP phones and for calls between SCCP phones. It is not supported for a mixture of SCCP and SIP phones; for example, it has no effect for calls from a SCCP phone to a SIP phone.

Examples

The following example shows how to disable SIP call transfer capabilities for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# no supplementary-service sip refer
```

The following example shows how to disable SIP call forwarding capabilities globally:

```
Router(config)# voice service voip
Router(conf-voi-serv)# no supplementary-service sip moved-temporarily
```

Related Commands

Command	Description
supplementary-service h450.2 (voice-service)	Globally enables H.450.3 capabilities for call transfer.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.

supported language

To configure Session Initiation Protocol (SIP) Accept-Language header support, use the **supported-language** command in voice service or dial peer voice configuration mode. To disable Accept-Language header support, use the **no** form of this command.

supported-language *language-code* **language-param** *qvalue*

no supported-language *language-code*

Syntax Description

language-code	Any of 139 languages designated by a two-letter ISO-639 country code.
qvalue	The priority of the language, with languages sorted in descending order according the assigned parameter value. Valid values include zero, one, or a decimal fraction in the range .001 through .999. Default is 1, the highest priority.
language-param	Specifies language preferences by associating a parameter with the language being configured.

Command Default

qvalue: 1

Command Modes

Dial peer voice configuration or Voice service configuration mode

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

To include the Accept-Language header in outgoing SIP INVITE messages, and enable Accept-Language header support on specific trunk groups with different language requirements, use dial peer voice configuration mode, which is enabled by the **dial-peer voice** command . To enable Accept-Language headers to be included in both SIP INVITE messages and OPTIONS responses, use voice service configuration mode, enabled by the **voice service pots** command. If both voice service and dial-peer voice mode accept-language support are configured, and there are no dial-peer matches, the outgoing INVITE message contains the voice service specified languages. Otherwise, the INVITE contains the dial-peer configured languages.

The SIP Accept-Language Header Support feature supports 139 languages which are designated by a two-letter ISO-639 country code. The following is a partial list of supported language codes and languages. To display a complete listing use the help command **supported-language ?**.

- **AR**—Arabic
- **ZH**—Chinese
- **EN**—English
- **EO**—Esperanto
- **DE**—German

- **EL**—Greek
- **HE**—Hebrew
- **GA**—Irish
- **IT**—Italian
- **JA**—Japanese
- **KO**—Korean
- **RU**—Russian
- **ES**—Spanish
- **SW**—Swahili
- **SV**—Swedish
- **VI**—Vietnamese
- **YI**—Yiddish
- **ZU**—Zulu

Examples

The following example configures Italian to be the preferred language, followed by Greek:

```
supported-language IT language-param .9
supported-language EL language-param .8
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers.

suppress

To suppress accounting for a specific call leg, use the **suppress** command in gateway accounting AAA configuration mode. To reenable accounting for that leg, use the **no** form of this command.

suppress [**pots** | **rotary** | **voip**]

no suppress [**pots** | **rotary** | **voip**]

Syntax Description

pots	(Optional) POTS call leg.
rotary	(Optional) Rotary dial peer.
voip	(Optional) VoIP call leg.

Command Default Accounting is enabled.

Command Modes Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to turn off accounting for a specific call leg.

If both incoming and outgoing call legs are of the same type, no accounting packets are generated.

Use the **rotary** keyword to suppress excess start and stop accounting records. This causes only one pair of records to be generated for every connection attempt through a dial peer.

Examples The following example suppresses accounting for the POTS call leg.

```
suppress pots
```

Related Commands

Command	Description
debug suppress rotary	Displays connection attempt statistics.
gw-accounting aaa	Enables VoIP gateway accounting.

suspend-resume (SIP)

To enable SIP Suspend and Resume functionality, use the **suspend-resume** command in SIP user agent configuration mode. To disable SIP Suspend and Resume functionality, use the **no** form of this command.

suspend-resume

no suspend-resume

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Session Initiation Protocol (SIP) gateways are now enabled to use Suspend and Resume. Suspend and Resume are basic functions of ISDN and ISDN User Part (ISUP) signaling procedures. A Suspend message temporarily halts communication (call hold), and a Resume message is received after a Suspend message and continues the communication.

Examples

The following example disables Suspend and Resume functionality:

```
Router(config)# sip-ua
Router(config-sip-ua)# no suspend-resume
```

Related Commands

Command	Description
show sip-ua status	Displays SIP UA status.
sip-ua	Enables the SIP user-agent configuration commands.

switchback interval

To set the amount of time that the digital signal processor (DSP) farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails, use the **switchback interval** command in SCCP Cisco CallManager configuration mode. To reset the amount of time to the default value, use the **no** form of this command.

switchback interval *seconds*

no switchback interval

Syntax Description

seconds	Timer value, in seconds. Range is 1 to 3600. Default is 60.

Command Default

60 seconds

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback interval value to meet your needs.

Examples

The following example sets the length of time the DSP farm waits to before polling the primary Cisco Unified CallManager to 120 seconds (2 minutes):

```
Router(conf-sccp-ccm)# switchback interval 120
```

Related Commands

Command	Description
connect interval	Specifies how many times a given profile attempts to connect to the specific CiscoUnified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchback method

To set the Cisco Unified CallManager switchback method, use the **switchback method** command in Skinny SCCP Cisco CallManager configuration mode. To reset to the default value, use the **no** form of this command.

switchback method {**graceful** | **guard** [*timeout-guard-value*] | **immediate** | **uptime** *uptime-timeout-value*}

no switchback method

Syntax Description

graceful	Selects the graceful switchback method.
guard	Selects the graceful with guard switchback method.
guard-timeout-value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.
immediate	Selects the immediate switchback method.
uptime	Selects the uptime-delay switchback method.
uptime-timeout-value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.

Command Default

Guard is the default switchback method, with a timeout value of 7200 seconds.

Command Modes

SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to set the Cisco Unified CallManager switchback method. When a switch-over happens with the secondary Cisco Unified CallManager initiates the switchback process with that higher-order Cisco Unified CallManager. The available switchback methods follow:

- graceful—The Cisco Unified CallManager switchback happens only after all the active sessions are terminated gracefully.
- guard—The Cisco Unified CallManager switchback happens either when the active sessions are terminated gracefully or when the guard timer expires, whichever happens first.
- immediate—Performs the Cisco Unified CallManager switchback to the higher order CiscoUnified CallManager immediately as soon as the timer expires, whether there is an active connection or not.
- uptime—Once the higher-order Cisco Unified CallManager comes alive, the uptime timer in initiated.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback method to meet your needs.

Examples

The following example sets the Cisco Unified CallManager switchback method to happen only after all the active sessions are terminated gracefully.

```
Router(config-sccp-ccm)# switchback method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchover method

To set the switchover method that the Skinny Client Control Protocol (SCCP) client uses when the communication link between the active Cisco Unified CallManager and the SCCP client goes down, use the **switchover method** command in SCCP Cisco CallManager configuration mode. To reset the switchover method to the default, use the **no** form of this command.

switchover method {**graceful** | **immediate**}

no switchover method

Syntax Description

graceful	Switchover happens only after all the active sessions are terminated gracefully.
immediate	Switches over to any one of the secondary Cisco Unified CallManager immediately.

Command Default Graceful

Command Modes SCCP Cisco CallManager configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines When the communication link between the active Cisco Unified CallManager and the SCCP client goes down the SCCP client tries to connect to one of the secondary Cisco Unified CallManagers using one of the following switchover methods:

- graceful—The Cisco Unified CallManager switchover happens only after all the active sessions are terminated gracefully.
- immediate—Regardless of whether there is an active connection or not the SCCP client switches over to one of the secondary Cisco Unified CallManagers immediately. If the SCCP Client is not able to connect to a secondary Cisco CUnified allManager, it continues polling for a CiscoUnified CallManager connection.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchover method to meet your needs.

Examples The following example sets the switchover method that the SCCP client uses to connect to a secondary Cisco Unified CallManager to happen only after all the active sessions are terminated gracefully:

```
Router (config-sccp-ccm)# switchover method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters the SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.

Cisco IOS Voice Commands: T

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the master index of commands or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Library.*

target carrier-id

To configure debug filtering for the target carrier ID, use the **target carrier-id** command in call filter match list configuration mode. To disable, use the **no** form of this command.

target carrier-id *string*

no target carrier-id *string*

Syntax Description

string	Alphanumeric identifier for the carrier ID.

Command Default No default behavior or values

Command Modes Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples The following example shows the voice call debug filter set to match target carrier ID 4321:

```
call filter match-list 1 voice
 target carrier-id 4321
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source carrier-id	Configure debug filtering for the source carrier ID.
source trunk-group-label	Configure debug filtering for a source trunk group.
target trunk-group-label	Configure debug filtering for a target trunk group.

target trunk-group-label

To configure debug filtering for a target trunk group, use the **target trunk-group-label** command in call filter match list configuration mode. To disable, use the **no** form of this command.

target trunk-group-label *group_number*

no target trunk-group-label *group_number*

Syntax Description

group_number	A value from 0 to 23 that identifies the trunk group.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match target trunk group 21:

```
call filter match-list 1 voice
 target trunk-group-label 21
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source carrier-id	Configure debug filtering for the source carrier ID.
source trunk-group-label	Configure debug filtering for a source trunk group.
target carrier-id	Configure debug filtering for the target carrier ID.

tbct clear call

To terminate billing statistics for one or more active Two B-Channel Transfer (TBCT) calls, use the **tbct clear call** command in privileged EXEC mode.

tbct clear call {**all** | *interface* [*call-tag*]}

Syntax Description

all	Active TBCT calls on all interfaces.
interface	Active TBCT calls on a specified interface. Range is platform-dependent.
call-tag	(Optional) A specific active TBCT call on the specified interface, as identified by the unique call tag number. Range is 1 to 4,294,967,295.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

- Use this command to manually clear a specific active call or a group of active calls, if, for instance, the ISDN switch goes down. You should not have to manually clear calls with this command unless there is a problem with the switch.
- This command terminates billing information that is being sent to the RADIUS server if, for some reason, the gateway did not receive a notify message from the switch that a call has cleared.
- To automatically clear calls after a specified duration, use the **tbct max call-duration** command.
- To determine the *interface* and *call-tag* arguments to use with this command, use the **show call active voice redirect** command.

Examples

The following example clears calls on T1 interface 6/0:

```
Router# tbct clear call T1-6/0
```

Related Commands

Command	Description
isdn supp-service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.

Command	Description
tbct max call-duration	Sets the maximum duration allowed for a call that is redirected using TBCT.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

tbct max call-duration

To set the maximum duration allowed for a call that is redirected using Two B-Channel Transfer (TBCT), use the **tbct max calls** command in global configuration mode. To reset to the default, use the **no** form of this command.

tbct max call-duration *minutes*

no tbct max call-duration

Syntax Description

minutes	Maximum duration, in minutes, allowed for a single TBCT call. Range is 1 to 9999, in recommended increments of 5 minutes. Default is no limit.

Command Default No limit

Command Modes Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

- Use this command to automatically clear stale calls, for instance if the PRI trunk goes down. To manually clear calls, use the **tbct clear call** command.
- Cisco recommends that you set the call duration in increments of 5 minutes.

Note The call duration limit set by this command is not precisely enforced; calls may not be cleared after the exact number of minutes specified by this command.

Examples The following example clears TBCT calls that last longer than 10 minutes:

```
tbct max call-duration 10
```

Related Commands

Command	Description
isdn supp-service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

tbct max calls

To set the maximum number of active calls that can use Two B-Channel Transfer (TBCT), use the **tbct max calls** command in global configuration mode. To reset to the default, use the **no** form of this command.

tbct max calls *number*

no tbct max calls

Syntax Description

number	Maximum number of currently active calls that can invoke TBCT at any one time. Range is 1 to 1,000,00. Default is no limit.

Command Default No limit, except as allowed by memory resources

Command Modes Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines Use this command to control memory resources on the gateway by limiting the amount of memory consumed by TBCT calls.

Examples The following example sets the maximum number of calls using TBCT to 500:

```
tbct max calls 500
```

Related Commands

Command	Description
isdn supp-service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max call-duration	Sets the maximum duration allowed for a call that is redirected using TBCT.

tdm-group

To configure a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect, use the **tdm-group** command in controller configuration mode. To delete a clear channel group, use the **no** form of this command.

tdm-group *tdm-group-no* **timeslot** *timeslot-list* [**type** {**e&m** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas**}]

no tdm-group *tdm-group-no* **timeslot** *timeslot-list* [**type** {**e&m** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas**}]

Syntax Description

tdm-group-no	TDM group number.
timeslot	Time-slot number.
timeslot-list	Time-slot list. T1 range is 1 to 24. E1 range is 1 to 15 and 17 to 31.
type	(Optional) (Valid only when the **mode cas** command is enabled.) Voice signaling type of the voice port. If configuring a TDM group for data traffic only, do not specify the type keyword. Choose from one of the following options: • **e&m**—E&M signaling • **fxs**—Foreign Exchange Station signaling (optionally, you can also specify loop-start or ground-start) • **fxo**—Foreign Exchange Office signaling (optionally, you can also specify loop-start or ground-start) • **fxs-melcas**—Foreign Exchange Station MEL CAS • **fxo-melcas**—Foreign Exchange Office MEL CAS • **e&m-melcas**—E&M Mercury Exchange Limited Channel-Associated signaling (MEL CAS) The MELCAS options apply only to E1 lines and are used primarily in the United Kingdom.

Command Default

No TDM group is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC38310.
12.1(1)T	This command was modified to include voice WAN interface cards (VWICs) for Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was modified for the OC-3/STM-1 ATM Circuit Emulation Service network module on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

The **tdm-group** command allows specific timeslots to switch from port 0 to port 1 and vice versa. This command is similar to the **channel-group** command, but it does not create a serial interface to terminate the specified channels.

Note Channel groups, CAS voice groups, DS0 groups, and TDM groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, DS0 groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.

Examples

The following example configures TDM group 1 to include timeslots 13 through 20:

```
controller T1 1
 tdm-group 1 timeslots 13-20
```

The following example configures TDM group number 20 on controller T1 1 to support Foreign Exchange Office (FXO) ground-start:

```
controller T1 1
 tdm-group 20 timeslot 20 type fxs ground-start
```

Related Commands

Command	Description
connect	Starts passage of data between ports for cross-connect TDM.

tech-prefix

To specify that a particular technology prefix be prepended to the destination pattern of a specific dial peer, use the **tech-prefix** command in dial peer configuration mode. To disable the defined technology prefix for this dial peer, use the **no** form of this command.

tech-prefix *number*

no tech-prefix

Syntax Description

number	Defines the numbers used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound (#) symbol is frequently used as the last character in a technology prefix. Valid characters are 0 though 9, the pound (#) symbol, and the asterisk (*).

Command Default

No technology prefix is defined.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on Cisco 2600 series and Cisco 3600 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Technology prefixes are used to distinguish between gateways that have specific capabilities within a given zone. In the exchange between the gateway and the gatekeeper, the technology prefix is used to select a gateway after the zone has been selected. Use the **tech-prefix** command to define technology prefixes.

Technology prefixes can be used as a discriminator so that the gateway can tell the gatekeeper that a certain technology is associated with a particular call (for example, 15# could mean a fax transmission), or a technology prefix can be used like an area code for more generic routing. No standard defines what the numbers in a technology prefix mean; by convention, technology prefixes are designated by a pound (#) symbol as the last character.

In most cases, there is a dynamic protocol exchange between the gateway and the gatekeeper that enables the gateway to inform the gatekeeper about technology prefixes and where to forward calls. If, for some reason, that dynamic registry feature is not in effect, you can statically configure the gatekeeper to query the gateway for this information by configuring the **gw-type-prefix** command on the gatekeeper. Use the **show gatekeeper gw-type-prefix command** to display how the gatekeeper has mapped the technology prefixes to local gateways.

Note Cisco gatekeepers use the asterisk (*) as a reserved character. If you are using Cisco gatekeepers, do not use the asterisk as part of the technology prefix.

Examples

The following example defines a technology prefix of 14# for the specified dial peer. In this example, the technology prefix means that the H.323 gateway asks the RAS gatekeeper to direct calls using the technology prefix of 14#.

```
dial-peer voice 10 voip
 destination-pattern 14...
 tech-prefix 14#
```

Related Commands

Command	Description
gw-type-prefix	Configures a technology prefix in the gatekeeper.
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.

tel-config to-hdr

To configure the To: Header (to hdr) Request URI to telephone (TEL) format for VoIP Session Initiation Protocol (SIP) calls, use the **tel-config to-hdr** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

tel-config to-hdr [**phone-context**]

no tel-config to-hdr

Syntax Description

phone-context	(Optional) Appends the phone context parameter to the TEL URL.

Command Default

The To: Header Request Line URIs are not configured to telephone format.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class tel-config to-hdr** command takes precedence over the **tel-config to-hdr** command configured in SIP configuration mode. However, if the **voice-class tel-config to-hdr** command is configured with the **system** keyword, the gateway uses the global settings configured by the **tel-config to-hdr** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example configures the To: header in TEL format, and appends the phone-context parameter to the header:

```
voice service voip
sip
 tel-config to-hdr phone-context
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class tel-config to-hdr	Configures the To: Header request URI to telephone format for dial-peer VoIP SIP calls.

telephony-service

To enter telephony-service configuration mode for configuring Cisco Unified CME, use the **telephony-service** command in global configuration mode. To remove the entire Cisco Unified CME configuration for SCCP IP phones, use the **no** form of this command.

telephony-service [**setup**]

no telephony-service

Syntax Description

setup	(Optional) Interactive setup tool for configuring Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME. **Note** This interactive Cisco CME setup tool is restricted to generating basic configuration files for Cisco Unified IP Phone 7910s, 7940s, and 7960s running SCCP protocol only.

Command Default

No Cisco Unified CME configuration for SCCP IP phones is present.

Command Modes

Global configuration (config)

Command History

Cisco IOS Release	Cisco Product	Modification
12.1(5)YD	Cisco ITS 1.0	This command was introduced.
12.2(8)T	Cisco ITS 2.0	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)ZJ	Cisco CME 3.0	The **setup** keyword was added.
12.3(4)T	Cisco CME 3.0	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command enters the telephony-service configuration mode for configuring system wide parameters for SCCP IP phones in Cisco Unified CME.

Note The voice-gateway system is tied to the telephony service. The **telephony-service** command must be configured before the voice-gateway system is configured; otherwise, the voice gateway is hidden from the user.

Use the **setup** keyword to start the interactive setup tool to automatically configure only Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME.

For alternate methods of automatically configuring Cisco Unified CME, including Cisco Unified IP Phone 7910s, 7940s, and 7960s and other Cisco Unified IP phones, see the *Cisco Unified CME Administrator Guide.*

The **setup** keyword is not stored in the router nonvolatile random-access memory (NVRAM).

If you attempt to use the **setup** option for a system that already has a telephony-service configuration, the command is rejected. To use the **setup** option after an existing telephony-service configuration has been created, first remove the existing configuration using the **no telephony-service** command.

Table 240 shows a sample dialog with the Cisco CME setup tool and explains possible responses to the Cisco CME setup tool prompts.

Table 240 Cisco CME Setup Tool Dialog Prompts

Cisco CME Setup Tool Prompt	Description

`Do you want to setup DHCP service for your IP phones? [yes/no]:`
 	
If you respond yes, you see the following prompts:
`IP network for telephony-service DHCP Pool:`
`Subnet mask for DHCP network :`
`TFTP Server IP address (Option 150) :`
`Default Router for DHCP Pool :`
	• **Yes**—Configures the Cisco Unified CME router to act as a Dynamic Host Configuration Protocol (DHCP) server, automatically providing IP addresses to your IP phones and provisioning the default gateway and TFTP IP addresses to be used by the phones. This method creates a single pool of IP addresses. If you need a pool for non-IP phones or if the Cisco router cannot act as the DHCP router, answer no and manually define the DHCP server.
	• **No**—Indicates that you have already configured DHCP or static IP addresses for the IP phones.

`Do you want to start telephony-service setup? [yes/no]:`	• **Yes**—Starts the interactive setup tool for configuring Cisco Unified IP Phone 7910s, 7940s, and 7960s. • **No**—Terminates the Cisco CME setup tool.

`Enter the IP source address for Cisco CallManager Express:`
 	
`Enter the Skinny Port for Cisco CallManager Express: [2000]:`
	IP address on which the router provides Cisco Unified CME services, usually the default gateway for the IP subnet that you are using for the IP phones, and the port for Skinny Client Control Protocol (SCCP) messages.

`How many IP phones do you want to configure : [0]:`	Enter the maximum number of IP phones that this Cisco Unified CME system will support. This number can be increased later, to the maximum allowed for this version and your router. **Note** The Cisco CME setup tool associates one number with each newly registering phone. You can manually add additional numbers on a phone at a later time.
`Do you want dual-line extensions assigned to phones? [yes for dual-line / no for single-line]:`	• **Yes**—Each newly registering IP phones is assigned a single number that is associated with a single phone button. The system generates a dual-line ephone-dn entry for each ephone-dn. • **No**—IP phones are linked directly to one or more PSTN trunk lines. Using keyswitch mode requires manual configuration in addition to using the Cisco CME setup tool. The system generates two ephone-dn entries for each ephone-dn, and they are both assigned to a single phone.

Table 240 Cisco CME Setup Tool Dialog Prompts (continued)

Cisco CME Setup Tool Prompt	Description
What language do you want on IP phones? 0 English 1 French 2 German 3 Russian 4 Spanish 5 Italian 6 Dutch 7 Norwegian 8 Portuguese 9 Danish 10 Swedish [0]:	Language for IP phone displays, selected from the list. • Default is 0, English.
Which Call Progress tone set do you want on IP phones : 0 United States 1 France 2 Germany 3 Russia 4 Spain 5 Italy 6 Netherlands 7 Norway 8 Portugal 9 UK 10 Denmark 11 Switzerland 12 Sweden 13 Austria 14 Canada [0]:	Locale for the tone set used to indicate call status or progress, selected from the list. • Default is 0, United States.
What is the first extension number you want to configure :[0]:	First number in pool of extension numbers to be created for IP phones connected to the Cisco router to be configured. • Starting with this number, remaining extension numbers are automatically configured in a contiguous manner. • This number must be compatible with your telephone number plan, and, if you use Direct Inward Dialing (DID) service, with public switched telephone network (PSTN) numbering requirements.
Do you have Direct-Inward-Dial service for all your phones? [yes/no]:	• **Yes**—If you have trunk access to public telephone service by ISDN or VoIP for all extension numbers. The system creates an appropriate dial plan. • **No**—If you have simple analog phone lines only (for example, foreign exchange office [FXO] interfaces) or if you have trunk access for some lines but not all lines.

Table 240 Cisco CME Setup Tool Dialog Prompts (continued)

Cisco CME Setup Tool Prompt	Description
If you answer yes to the previous question, you see the following prompt: `Enter the full E.164 number for the first phone:`	Complete 10-digit telephone number, including area code, that corresponds to the first extension number.
`Do you want to forward calls to a voice message service? [yes/no]:`	• **Yes**—To forward calls to a single voice message service number when an IP phone is busy or does not answer. All phone extensions forward their calls to the same voice message service pilot number. • **No**—Not to forward calls to a single voice message service number. Answer **no** if you do not have a voice message system or if you want to customize call-forwarding behavior for each extension.
If you answer yes to the previous question, you see the following prompt: `Enter the extension or pilot number of the voice message service:`	Voice message service pilot number. • This step can be ignored during the setup dialog and manually configured later.
`Call forward No Answer Timeout: [18]:`	Timeout, in seconds, after which to forward calls to voice mail if they are not answered. • Default is 18.
`Do you wish to change any of the above information? [yes/no]:`	• **Yes**—Starts the dialog over again without implementing any of the answers that you previously gave. • **No**—Uses specified values to automatically build basic configuration for Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME.

Examples

The following example shows how to enter telephony-service configuration mode for manually configuring Cisco Unified CME. This example also configures the maximum number of phones to 12:

```
Router(config)# telephony-service
Router(config-telephony)# max-ephones 12
```

The following example shows how to start the Cisco CME setup tool:

```
Router(config)# telephony-service setup
```

telephony-service ccm-compatible (H.323 voice-class)

To enable, for an individual dial peer, the detection of a Cisco CallManager system in the network and allow the exchange of calls, use the **telephony-service ccm-compatible** command in voice-class configuration mode. To disable the detection capability and the exchange of calls on an individual dial peer, use the **no** form of this command.

telephony-service ccm-compatible

no telephony-service ccm-compatible

Syntax Description

This command has no arguments or keywords.

Command Default

Detection of Cisco CallManager systems is enabled.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command is used with Cisco CallManager Express (Cisco CME) 3.1 or a later version.

When a voice class that contains this command is applied to a dial peer, this command enables detection of and call exchange with Cisco CallManager for all calls from that dial peer. Use the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode to create a voice class to apply this capability globally. If the capability is specified at both the global and dial-peer level, the dial-peer setting has precedence for that dial peer.

Examples

The following example globally enables detection of Cisco CallManager systems in the network, creates voice class 4 to disable the capability on individual dial peers, and applies voice class 4 to dial peer 36. Although the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode is not required because this condition is the default, the command is shown here for illustration purposes.

```
Router(config)# voice service voip
Router(config-voi-serv)# h323
Router(conf-serv-h323)# telephony-service ccm-compatible
Router(conf-serv-h323)# exit
Router(config-voi-serv)# exit
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
telephony-service ccm-compatible (H.323 voice-service)	Globally enables detection of Cisco CallManager in a network for all dial peers.
voice class h323	Creates an H.323 voice class to apply to a dial peer.
voice-class h323	Applies an H.323 voice class to a dial peer.

telephony-service ccm-compatible (H.323 voice-service)

To globally enable the detection of a Cisco CallManager system in the network and allow the exchange of calls, use the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode. To disable the detection capability and the exchange of calls globally, use the **no** form of this command.

telephony-service ccm-compatible

no telephony-service ccm-compatible

Syntax Description

This command has no arguments or keywords.

Command Default

Detection of Cisco CallManager systems is enabled.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command is used with Cisco CallManager Express (Cisco CME) 3.1 or a later version.

This command globally enables call exchange with Cisco CallManager for all calls from this router. Use the **telephony-service ccm-compatible** command in voice-class configuration mode to create a voice class in order to apply this capability to an individual dial peer. If the capability is specified at both the global and dial-peer level, the dial-peer setting has precedence for that dial peer.

Examples

The following example globally enables detection of Cisco CallManager systems in the network, creates voice class 4 to disable the capability on individual dial peers, and applies voice class 4 to dial peer 36. Although the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode is not required because this condition is the default, the command is shown here for illustration purposes.

```
Router(config)# voice service voip
Router(config-voi-serv)# h323
Router(conf-serv-h323)# telephony-service ccm-compatible
Router(conf-serv-h323)# exit
Router(config-voi-serv)# exit
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
h323	Enters H.323 voice-service configuration mode.
telephony-service ccm-compatible (H.323 voice-class)	Enables Cisco CallManager detection in a network by individual dial peers.
voice service voip	Enters voice-service configuration mode.

Related Commands

Command	Description
test vrm busyout	Busy outs a specific DSP or channels on a specific DSP.

text relay modulation

To configure the TTY modulation used on the gateway for Cisco text relay for Baudot text phones, use the **text relay modulation** command in dial peer configuration mode or voice-service configuration mode. To disable text relay modulation, use the **no** form of this command.

text relay modulation {baudot45.45 | baudot50} {autobaud-on | autobaud-off}

no text relay modulation

Syntax Description

baudot45.45	Configures baudot 45.45 TTY modulation. This is the default baud rate.
baudot50	Configures baudot 50 TTY modulation.
autobaud-on	Enables the digital signal processors (DSPs) to autodetect the baud rate. This is the default autobaud setting.
autobaud-off	Disables the DSP capability to autodetect the baud rate.

Command Default

The TTY modulation is **baudot45.45 autobaud-on**.

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You must select a baud rate and enable or disable the autobaud functionality on the DSP.

- Use this command in voice-service configuration mode to set the TTY modulation globally. A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.
- Use this command in dial peer configuration mode to set the TTY modulation for calls that match a specific dial peer. The dial peer configuration takes precedence over the global configuration.

Examples

The following example shows how to globally set the text relay TTY modulation to Baudot 50:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay modulation baudot50 autobaud-off
```

The following example shows how to set the text relay TTY modulation to Baudot 50 for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay modulation baudot50 autobaud-off
```

Related Commands

Command	Description
text relay protocol	Configures the system-wide protocol type for text packets transmitted between gateways.
text relay rtp	Configures the RTP payload type and redundancy level.

text relay protocol

To enable Cisco text relay for Baudot text phones, use the **text relay protocol** command in dial peer configuration mode or voice-service configuration mode. To disable text relay capabilities, use the **no** form of this command.

text relay protocol [cisco | system]

no text relay protocol

Syntax Description

cisco	(Optional) Uses the Cisco proprietary text relay protocol.
system	(Optional; dial peer configuration only) Uses the global configuration settings.

Command Default

The text relay protocol is disabled.

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

- Use this command in voice-service configuration mode to enable text relay globally for H.323, SIP, and MGCP. A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.
- Use this command in dial peer configuration mode to enable text relay for calls that match a specific dial peer. The dial peer configuration takes precedence over the global configuration.

Examples

The following example shows how to enable text relay for all VoIP calls on the gateway:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay protocol cisco
```

The following example shows how to enable text relay for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay protocol cisco
```

Related Commands

Command	Description
text relay modulation	Configures the TTY modulation on the gateway.
text relay rtp	Configures the RTP payload type and redundancy level.

text relay rtp

To configure the Real-Time Transport Protocol (RTP) payload type and redundancy level for Cisco text relay for Baudot text phones, use the **text relay rtp** command in dial peer configuration mode or voice-service configuration mode. To disable the text relay RTP payload type and redundancy level, use the **no** form of this command.

text relay rtp {payload-type {*value* **| default} {redundancy** *level***}**

no text relay rtp

Syntax Description

payload-type {*value* **| default***}*	The RTP payload is the data transported by RTP in a packet. • The *value* range is 98 to 117 for dynamic RTP payload types. • The **default** value is 119, which is a static payload type.
redundancy *level*	Use the redundancy option to repeat data for redundancy and to lower the risk of packet loss. The redundancy level is the number of redundant text packets sent across the VoIP network. The range is 1 to 3. The default value is 2.

Command Default

Text relay RTP is disabled.

Command Modes

Dial peer configuration
Voice-service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When using the **text relay rtp** command, you can either configure the **payload-type**, or the redundancy level, or both.

- Use this command in voice-service configuration mode to set the RTP payload type and redundancy level globally for H.323, SIP, and MGCP. A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.
- Use this command in dial peer configuration mode to set the RTP payload type and redundancy level for calls that match a specific dial peer. The dial peer configuration takes precedence over the global configuration.

Examples

The following example shows how to globally configure text relay RTP payload type 117 and redundancy level 2:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay rtp payload-type 117 redundancy 2
```

The following example shows how to configure the default text relay RTP payload type and redundancy level 1 for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay rtp payload-type default redundancy 1
```

Related Commands

Command	Description
text relay modulation	Configures the TTY modulation on the gateway.
text relay protocol	Configures the system-wide protocol type for text packets transmitted between gateways.

tgrep address-family

To set the address family to be used on a local dial peer, use the **tgrep address-family** command in dial peer configuration mode. To return to the global setting, use the **no** form of this command.

tgrep address family {e164 | decimal | penta-decimal}

no tgrep address family {e164 | decimal | penta-decimal}

Syntax Description

e164	E.164 address family.
decimal	Decimal address family
penta-decimal	Penta-decimal address family

Command Default No default behavior or values.

Command Modes Dial peer configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines The E. 164 address family is used if the telephony network is a public telephony network. Decimal and pentadecimal options can be used to advertise private dial plans. For example if a company wants to use TRIP in within their enterprise telephony network using 5-digit extensions, then the gateway would advertise the beginning digits of their private numbers as a decimal address family. These calls cannot be sent out of the company's private telephony network because they are not E.164-compliant.

The pentadecimal family allows numbers 0 through 9 and alphabetic characters A through E and can be used in countries where letters are also carried in the called number.

Examples The following example shows that POTS dial peer 10 has the address family set for E.164 addresses:

```
Router(config)# dial-peer voice pots 10
Router(config-dial-peer)# tgrep address family e164
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.

tgrep advertise (dial peer)

To set the attributes for advertisement of the prefix on this dial peer or to disable advertisement on this dial peer altogether, use the **tgrep advertise** command in dial peer configuration mode. To return to using the global setting, use the **no** form of this command.

tgrep advertise [**csr**] [**ac**] [**tc**] [**carrier** | **trunk-group**] [**disable**]

no tgrep advertise [**csr**] [**ac**] [**tc**] [**carrier** | **trunk-group**] [**disable**]

Syntax Description

csr	Call success rate
ac	Available circuits
tc	Total circuits
carrier	Carrier code address family
trunk-group	Trunk group address family
disable	Disables advertisement of this dial peer

Command Default

Prefix advertisement is not sent.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

When only **tgrep advertise** is entered, the dial peer is advertised without any other attribute.

When **no tgrep advertise** is used on the dial peer, the dial peer inherits the attributes set in the global **advertise** command.

When the global **no advertise** command is used, it forbids advertisement of that particular address family altogether. The **tgrep advertise** command has no effect until the advertisement of the address family is enabled globally.

Examples

The following example shows a TGREP advertisement that sends call success rate, available circuits, total circuits, and carrier address family attribute information:

```
Router(config)# dial-peer voice pots 10
Router(config-dial-peer)# tgrep advertise csr ac tc carrier
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.

tgrep advertise (trunk group)

To turn on the advertisement of this trunk group for resource availability and other carrier information, use the **tgrep advertise** command in trunk group configuration mode. To turn off local trunk group advertisement and use the global setting, use the **no** form of this command.

tgrep advertise [**csr**] [**ac**] [**tc**] [**disable**]

no tgrep advertise [**csr**] [**ac**] [**tc**] [**disable**]

Syntax Description

csr	Call success rate.
ac	Available circuits.
tc	Total circuits.
disable	Disables advertisement on the trunk group.

Command Default Trunk group advertisement is not sent

Command Modes Trunk group configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines When only **tgrep advertise** is entered, the trunk group is advertised without any other attribute. When **no tgrep advertise** is used, the trunk group uses the global setting configured with the **advertise** command in TGREP configuration mode. To turn off advertisement of this trunk group, the **disable** keyword should be used.

There is a subtle difference between the **no** form of this command and the **no** form of the global **advertise** command. When **no tgrep advertise** is used on the trunk group, the trunk group inherits the attributes set in the global **advertise** command.

When the global **no advertise** command is used, it forbids advertisement of that particular address family altogether. The **tgrep advertise** command has no effect until the advertisement of the address family is enabled globally.

When the **carrier** keyword is used, the carrier defined under the trunk group assumes the configuration. Because multiple trunk groups can have the same carrier defined, the same configuration will show up under all trunk groups that have the same carrier defined. When the **no tgrep advertise carrier** command is used to revert to the global carrier configuration for the carrier under this trunk group, the same will happen to all the trunk groups who have the same carrier defined under them.

Note This command overrides the attributes set for advertisement using the global **advertise (tgrep)** command.

Examples

The following example shows that trunk group 101 has been configured to send a TGREP advertisement that sends call success rate, available circuits, total circuits, and prefix attribute information:

```
Router(config)# trunk group 101
Router(config-dial-peer)# tgrep advertise csr ac tc carrier
```

Related Commands

Command	Description
advertise (tgrep)	Turns on reporting for a specified address family.
trunk group	Defines the trunk group and enters trunk group configuration mode.

tgrep local-itad

To enable Telephony Gateway Registration Protocol (TGREP) on the gateway and enter TGREP configuration mode, use the **tgrep local-itad** command in global configuration mode. To disable the configuration on the gateway, use the **no** form of this command.

tgrep local-itad [*itad-number*]

no tgrep local-itad [*itad-number*]

Syntax Description

itad-number	(Optional) IP Telephony Administrative Domain (ITAD) number associated with the gateway. The range is from 1 to 4294967295.

Command Default

TGREP is disabled on the gateway.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows how to enable TGREP for ITAD number 1234:

```
Router# enable
Router(config)# tgrep local-itad 1234
```

Related Commands

Command	Description
address-family	Sets the global address family to be used on all dial peers.
advertise (tgrep)	Turns on reporting for a specified address family.
neighbor	Creates a TGREP session with another device.

threshold noise

To configure a noise threshold for incoming calls, use the **threshold noise** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

threshold noise {*value*}

no threshold noise {*value*}

Syntax Description

value	Number that establishes a noise threshold. Valid values are from -30 to -90 decibels (dBs). The default is -62 dB.

Command Default

-62 dB

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(13b)	This command was introduced on the following platforms: Cisco 1700 Cisco 1751, Cisco 2600 (with and without the NM-HDA), Cisco 3600 (with and without the NM-HDA), Cisco 7200 (with and without the NM-HDA), Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.2(16)	This command was integrated into Cisco IOS Release 12.2(16).

Usage Guidelines

Cisco voice activity detection (VAD) has two layers: application programming interface (API) layer and processing layer. There are 3 states that the processing layer classifies incoming signals: speech, unknown, and silence. The state of the incoming signals is determined by the noise threshold.

In earlier Cisco IOS releases, the noise threshold is fixed between -62 dB and -78 dB. If the voice level is below the noise threshold, then the signal is classified as silence. If the incoming signal cannot be classified, the variable thresholds that are computed with the statistics of speech and noise that VAD gathers is used to make a determination. If the signal still cannot be classified, then it is marked as unknown. The final decision is made by the API. For applications such as hoot-n-holler, you could have the noise create unwanted spurious packets (for example, a voice stream) taking up bandwidth.

With Cisco IOS Release 12.2(16), the noise threshold is configurable using the **threshold noise** command.

Examples

The following sample configuration shows a noise threshold level of -50 dB:

```
voice-port 1/0/0
 threshold noise -50
```

timeout (auto-config application)

To configure the download timeout value for an auto-configuration application, use the **timeout** command in auto-config application configuration mode. To reset to the default, use the **no** form of this command.

timeout *time-in-seconds*

no timeout

Syntax Description

time-in-seconds	Specifies the download timeout value in seconds. The range is from 0 to 3600. The default is 180.

Command Default

The default value is 180 seconds.

Command Modes

Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

A value of 0 specifies continuous download retry.

Examples

The following example shows the **timeout** command used to specify continuous retry for downloading an auto-configuration application:

```
Router(auto-config-app)# timeout 0
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCPapplication.
show auto-config	Displays the current status of auto-configuration applications.

timeout leg3

To set the timeout value for a leg 3 AAA preauthentication request, use the **timeout leg3** command in AAA preauthentication configuration mode. To return the timeout value to its default, use the **no** form of this command.

timeout leg3 *milliseconds*

no timeout leg3 *milliseconds*

Syntax Description

milliseconds	Timeout value for leg 3 preauthentication, in milliseconds. Range is from 100 to 1000. The default is 100.

Command Default

100 milliseconds.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

If the timeout timer expires before AAA has responded to a preauthentication request, the call is rejected.

The term leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following example sets the timeout for a leg 3 AAA preauthentication request to 250 milliseconds:

```
Router(config)# aaa preauth
Router(config-preauth)# timeout leg3 250
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

timeout ptt

To specify a maximum time for transmitting or receiving a voice packet, use the **timeout ptt** command in voice-port configuration mode. To return to the default, use the **no** form of this command.

timeout ptt {**rcv** | **xmt**} *minutes*

no timeout ptt {**rcv** | **xmt**} *minutes*

Syntax Description

rcv	Applies the specified time limit to the reception of voice packets.
xmt	Applies the specified time limit to the transmission of voice packets.
minutes	Maximum time, in minutes, allowed for transmitting or receiving a voice packet. Range is integers from 1 to 30.

Command Default

minutes: 0 minutes

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timeout ptt** command is available on an ear and mouth (E&M) analog or digital voice port only if the signal type for that port is Land Mobile Radio (LMR). The purpose of this command is to limit extended radio transmission. When the time limit configured with this command expires, the radio transmitter unkeys, so that listeners on the channel cannot hear the speaker, even if the speaker continues to talk. When the speaker unkeys the radio, the timer is reactivated.

Examples

The following example specifies a maximum time of 10 minutes for transmitting a voice packet:

```
voice-port 1/0/0
 timeout ptt xmt 10
```

timeout tcrit

To configure the critical timeout value, T(critical), for the interdigit timer used in digit map matching, use the **timeout tcrit** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tcrit *tcrit-value*

no timeout tcrit

Syntax Description

tcrit-value	Critical timeout value, T(critical), in seconds. Range is from 1 to 600. Default is 4.

Command Default 4 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The interdigit timer is used when matching a digit map, which is a representation of the number and type of digits that a gateway can expect to collect in a buffer, based on the network dial plan. The interdigit timer is started when the first digit is entered and is restarted after each new digit is entered, until a digit map match or mismatch occurs.

The interdigit timer takes on one of two values, T(partial) or T(critical). When at least one more digit is required to make a match to any of the patterns in the digit map, the value of T(partial) is used for the timer. If a timer is all that is required to produce a match according to the digit map, T(critical) is used for the timer.

When the interdigit timer is used without a digit map, it takes on the value T(critical). It is started immediately and is simply canceled (but not restarted) as soon as a digit is entered.

Examples The following example sets the T(critical) value to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tcrit 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tpar	Configures the MGCP partial timeout value, T(partial), for the interdigit timer used in digit map matching.

timeout tdinit

To configure the initial waiting delay value (Tdinit) for the disconnected procedure, use the **timeout tdinit** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdinit *tdinit-value*

no timeout tdinit

Syntax Description

tdinit-value	Initial waiting delay (Tdinit) for the disconnected procedure, in seconds. The disconnected timer is initialized to a randomly selected value between 0 and Tdinit. Range is from 1 to 30. Default is 15.

Command Default

15 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit** command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the disconnected procedure for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin** command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax** command.

Examples

The following example sets the initial waiting delay value (Tdinit) to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdinit 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdmax	Configures the maximum timeout for the MGCP disconnected procedure.
timeout tdmin	Configures the minimum timeout for the MGCP disconnected procedure.

timeout tdmax

To configure the maximum timeout value (Tdmax) for the disconnected procedure, use the **timeout tdmax** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdmax *tdmax-value*

no timeout tdmax

Syntax Description

tdmax-value	Maximum timeout value (Tdmax) for the disconnected procedure, in seconds. Range is from 300 to 600. The default is 600.

Command Default 600 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit** command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the disconnected procedure for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin** command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax** command.

Examples The following example sets the maximum timeout value (Tdmax) to 450 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdmax 450
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdinit	Configures the initial timeout for the MGCP disconnected procedure.
timeout tdmin	Configures the minimum timeout for the MGCP disconnected procedure.

timeout tdmin

To configure the minimum timeout value (Tdmin) for the disconnected procedure, use the **timeout tdmin** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdmin *tdmin-value*

no timeout tdmin

Syntax Description

tdmin-value	Minimum timeout (Tdmin) for the disconnected procedure, in seconds. Range is from 1 to 30. The default is 15.

Command Default 15 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit** command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the disconnected procedure for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin** command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax** command.

Examples The following example sets the minimum timeout value (Tdmin) to 20 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdmin 20
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdinit	Configures the initial timeout for the MGCP disconnected procedure.
timeout tdmax	Configures the maximum timeout for the MGCP disconnected procedure.

timeout thist

To configure the packet storage timeout value (Thist), use the **timeout thist** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout thist *thist-value*

no timeout thist

Syntax Description

thist-value	Package storage timeout (Thist), in seconds. Range is from 1 to 60. The default is 30.

Command Default 30 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

MGCP messages are carried over User Datagram Protocol (UDP), and are therefore subject to packet loss. When a response to a message is not received promptly, the sender retransmits the message. The gateway keeps in memory a list of the responses it has sent for the number of seconds in the Thist timeout value. The gateway also keeps a list of the messages currently being processed, with their transaction identifiers, to prevent processing or acknowledging the same message more than once.

Examples The following example sets the packet storage timeout value (Thist) to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout thist 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

timeout tone busy

To configure the busy-tone timeout value, use the **timeout tone busy** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone busy *busy-tone-value*

no timeout tone busy

Syntax Description

busy-tone-value	Busy-tone timeout, in seconds. Range is from 1 to 600. The default is 30.

Command Default

30 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the busy-tone timeout value when the call agent does not provide a timeout value associated with the request to generate a busy tone signal.

Examples

The following example sets the busy tone timeout value to 45 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone busy 45
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone cot1

To configure the continuity1 (cot1) tone timeout value, use the **timeout tone cot1** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone cot1 *cot1-tone-value*

no timeout tone cot1

Syntax Description

cot1-tone-value	Continuity1 (cot1) tone timeout, in seconds. Range is from 1 to 600. The default is 3.

Command Default 3 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the continuity1 (cot1) tone timeout value when the call agent does not provide a timeout value associated with the request to generate a cot1 tone signal.

Continuity1 and continuity2 tone signals are used in Integrated Services Digital Networks User Part (ISUP) calls to determine that a call path has been established before connecting a call. The call agent is provisioned to know which test to apply to a given endpoint.

Examples The following example sets the continuity1 tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone cot1 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tone cot2	Sets the continuity2 tone timeout value for MGCP.

timeout tone cot2

To configure the continuity2 (cot2) tone timeout value, use the **timeout tone cot2** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone cot2 *cot2-tone-value*

no timeout tone cot2

Syntax Description

cot2-tone-value	Continuity2 (cot2) tone timeout, in seconds. Range is from 1 to 600. The default is 3.

Command Default 3 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the continuity2 (cot2) tone timeout value when the call agent does not provide a timeout value associated with the request to generate a cot2 tone signal.

Continuity1 and continuity2 tone signals are used in Integrated Services Digital Networks User Part (ISUP) calls to determine that a call path has been established before connecting a call. The call agent is provisioned to know which test to apply to a given endpoint.

Examples The following example sets the continuity2 tone timeout value to 50 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone cot2 50
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tone cot1	Sets the continuity1 tone timeout value for MGCP.

timeout tone dial

To configure the dial tone timeout value, use the **timeout tone dial** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone dial *dial-tone-value*

no timeout tone dial

Syntax Description

dial-tone-value	Dial tone timeout value, in seconds. Range is from 1 to 600. The default is 16.

Command Default

16 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the dial tone timeout value when the call agent does not provide a timeout value associated with the request to generate a dial tone signal.

Examples

The following example sets the dial tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone dial 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone dial stutter

To configure the stutter dial tone timeout value, use the **timeout tone dial stutter** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone dial stutter *stutter-value*

no timeout tone dial stutter

Syntax Description

stutter-value	Timeout value for the stutter dial tone, in seconds. Range is from1 to 600. The default is 16.

Command Default 16 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the stutter dial tone timeout value when the call agent does not provide a timeout value associated with the request to generate a stutter dial tone signal.

Examples The following example sets the stutter dial tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone dial stutter 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone mwi

To configure the timeout value for the message-waiting indicator tone, use the **timeout tone mwi** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone mwi *mwi-tone-value*

no timeout tone mwi

Syntax Description

mwi-tone-value	Message-waiting-indicator (MWI) tone timeout value, in seconds. Range is from 1 to 600. The default is 16.

Command Default 16 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the *mwi-tone-value* when the call agent does not provide a timeout value for a request to generate the message-waiting indicator tone signal.

Examples The following example sets the timeout value for the message-waiting indicator tone to 100 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone mwi 100
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone network

To configure the network congestion tone timeout value, use the **timeout tone network** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone network {**congestion** | **busy**} *tone-value*

no timeout tone network

Syntax Description

congestion	Timeout for network congestion.
busy	Timeout for network busy.
tone-value	Tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.4(9)T	The **busy** keyword was introduced.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the tone timeout value when the call agent does not provide a timeout value associated with the request to generate a network congestion or network busy tone signal.

Examples

The following example sets the network congestion tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone network congestion 240
```

The following example shows the network busy timeout value being set to 300 seconds.

Router(config)# **mgcp profile sample**

```
Router(config-mgcp-profile)# timeout tone network busy 300
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone reorder

To configure the reorder tone timeout value, use the **timeout tone reorder** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone reorder *reorder-tone-value*

no timeout tone reorder

Syntax Description

reorder-tone-value	Reorder-tone timeout value, in seconds. Range is from 1 to 600. The default is 30.

Command Default

30 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the reorder tone timeout value when the call agent does not provide a timeout value associated with the request to generate a reorder tone signal.

Examples

The following example sets the reorder tone timeout value to 60 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone reorder 60
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringback

To configure the ringback tone timeout value, use the **timeout tone ringback** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringback *ringback-tone-value*

no timeout tone ringback

Syntax Description

ringback-tone-value	Ringback-tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default 180 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the ringback tone timeout value when the call agent does not provide a timeout value associated with the request to generate a ringback tone signal.

Examples The following example sets the ringback tone timeout value to 120 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringback 120
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringback connection

To configure the timeout value for the ringback tone on connection, use the **timeout tone ringback connection** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringback connection *connect-tone-value*

no timeout tone ringback connection

Syntax Description

connect-tone-value	Timeout value for the ringback tone on connection, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses this value when the call agent does not provide a timeout value associated with the request to generate the ringback tone signal on connection.

Examples

The following example sets the timeout value for the ringback tone on connection to 120 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringback connection 120
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringing

To configure the ringing tone timeout value, use the **timeout tone ringing** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringing *ringing-tone-value*

no timeout tone ringing

Syntax Description

ringing-tone-value	Ringing tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default 180 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the ringing tone timeout value when the call agent does not provide a timeout value associated with the request to generate a ringing tone signal.

Examples The following example sets the ringing tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringing 240
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringing distinctive

To configure the distinctive ringing tone timeout value, use the **timeout tone ringing distinctive** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringing distinctive *distinct-tone-value*

no timeout tone ringing distinctive

Syntax Description

distinct-tone-value	Distinctive-ringing tone timeout value, in seconds. Range is from 1 to 600. the default is 180.

Command Default 180 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the distinctive ringing tone timeout value when the call agent does not provide a timeout value associated with the request to generate a signal for distinctive ringing.

Examples The following example sets the distinctive ringing tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringing distinctive 240
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tpar

To configure the partial timeout value, T(partial), for the interdigit timer used in digit map matching, use the **timeout tpar** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tpar *tpar-value*

no timeout tpar

Syntax Description

tpar-value	Partial timeout value, T(partial), in seconds. Range is from 1 to 60. The default is 16.

Command Default 16 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The interdigit timer is used when matching digit maps. It is started when the first digit is entered, and is restarted after each new digit is entered, until a digit map match or mismatch occurs.

The interdigit timer takes on one of two values, T(partial) or T(critical). When at least one more digit is required to make a match to any of the patterns in the digit map, the value of T(partial) is used for the timer. If a timer is all that is required to produce a match according to the digit map, T(critical) is used for the timer.

When the interdigit timer is used without a digit map, it takes on the value T(critical). It is started immediately and is simply canceled (but not restarted) as soon as a digit is entered.

Examples The following example sets the partial timeout value to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tpar 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tcrit	Configures the MGCP critical timeout value, T(critical), for the interdigit timer used in digit map matching.

timeout tsmax

To configure the maximum timeout value after which MGCP messages are removed from the retransmission queue, use the **timeout tsmax** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tsmax *tsmax-value*

no timeout tsmax

Syntax Description

tsmax-value	Timeout value for MGCP messages to be removed from the retransmission queue, in seconds. Range is from 1 to 100. The default is 20.

Command Default 20 seconds

Command Modes MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the *tsmax-value* argument to determine how long to store MGCP messages before they are removed from the retransmission queue.

Examples The following example sets the timeout value for the maximum retransmission of MGCP messages to 45 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tsmax 45
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeouts call-disconnect

To configure the delay time for which a Foreign Exchange Office (FXO) voice port waits before disconnecting an incoming call after disconnect tones are detected, use the **timeouts call-disconnect** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts call-disconnect {*seconds* | **infinity**}

no timeouts call-disconnect

Syntax Description

seconds	Duration in seconds for which an FXO voice port stays in the connected state after the voice port detects a disconnect tone. Range is 1 to 120. The default is 60.
infinity	Disables disconnect supervision. The voice port does not disconnect when a disconnect tone is detected.

Command Default 60 seconds

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(9)T	This command was introduced on Cisco 3600 series routers.
12.0(4)T	This command was introduced on Cisco 3600 series routers.
12.2(2)T	This command was implemented on Cisco 1750, Cisco 2600 series, and Cisco MC3810. The **infinity** keyword was added.

Usage Guidelines Use this command to change the time for which an FXO voice port remains connected after the calling party hangs up, when a call is not answered. Use of the **infinity** keyword is not recommended for disabling the disconnect supervision feature.

Examples The following example configures voice port 0/0/1 to remain connected for 3 seconds while a disconnect tone is received by the voice port:

```
voice-port 0/0/1
 timeouts call-disconnect 3
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

timeouts wait-release	Specifies the delay time for releasing the calling voice port after a disconnect tone is received from the called voice port.
timing delay-duration	Configures the delay dial signal duration for a specified voice port.

timeouts initial

To configure the initial digit timeout value for a specified voice port, use the **timeouts initial** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts initial *seconds*

no timeouts initial *seconds*

Syntax Description

seconds	Initial timeout duration, in seconds. Range is 0 to 120. The default is 10.

Command Default

10 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

Use the **timeouts initial** command to specify the number of seconds for which the system waits for the caller to input the first digit of the dialed digits. The timeouts initial timer is activated when the call is accepted and is deactivated when the caller inputs the first digit. If the configured timeout value is exceeded, the caller is notified through the appropriate tone and the call is terminated.

To disable the timeouts initial timer, set the *seconds* value to 0.

Examples

The following example sets the initial digit timeout value to 10 seconds:

```
voice-port 1/0/0
 timeouts initial 10
```

Related Commands

Command	Description
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

timeouts interdigit (voice port)

To configure the interdigit timeout value for a specified voice port, use the **timeouts interdigit** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts interdigit *seconds*

no timeouts interdigit *seconds*

Syntax Description

seconds	Interdigit timeout duration, in seconds. Range is 0 to 120. The default is 10.

Command Default

10 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

Use this command to specify the number of seconds for which the system waits (after the caller inputs the initial digit) for the caller to input a subsequent digit of the dialed digits. The timeouts interdigit timer is activated when the caller inputs a digit and is restarted each time the caller inputs another digit until the destination address is identified. If the configured timeout value is exceeded before the destination address is identified, the caller is notified through the appropriate tone and the call is terminated.

To disable the timeouts interdigit timer, set the *seconds* value to 0.

Examples

The following example sets the interdigit timeout value on the Cisco 3600 series for 10 seconds:

```
voice-port 1/0/0
 timeouts interdigit 10
```

The following example sets the interdigit timeout value on the Cisco MC3810 for 10 seconds:

```
voice-port 1/1
 timeouts interdigit 10
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.

timeouts power-denial

To set the duration of the power denial timeout for the specified FXS voice port, use the **timeouts power-denial** command in voice-port configuration mode. To reset the timeout to the default, use the **no** form of this command.

timeouts power-denial *ms*

no timeouts power-denial

Syntax Description

ms	Length of power denial, in milliseconds (ms). Range: 0 to 2500. Default: 750.

Command Default

Default is 750 ms.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(2)T	The maximum value of the *ms* argument was increased from 1500 to 2500.

Usage Guidelines

This command sets the duration of the power denial that the voice gateway applies to the FXS port when a call disconnects. During the power denial duration the caller hears silence. To disable the power denial on a port, use the **no supervisory disconnect lcfo** command.

Examples

The following example sets the power-denial duration to 500 ms:

```
voice-port 2/0
 timeouts power-denial 500
```

Related Commands

Command	Description
supervisory disconnect lcfo	Signals a disconnect on an FXS loop-start port by applying a power denial using a LCFO.

timeouts ringing

To configure the timeout value for ringing, use the **timeouts ringing** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts ringing {*seconds* | **infinity**}

no timeouts ringing

Syntax Description

seconds	Duration, in seconds, for which a voice port allows ringing to continue if a call is not answered. Range is 5 to 60000. Default is 180 for nonSCCP-controlled ports.
infinity	Ringing continues until the caller goes on-hook. Default value for SCCP-controlled analog ports.

Command Default

infinity for SCCP-controlled analog ports; 180 seconds for all other ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.4(11)T	The command default value was increased from 180 seconds to infinity for SCCP-controlled analog ports.

Usage Guidelines

This command allows you to limit the length of time for which a caller can continue ringing a telephone when there is no answer.

In Cisco IOS Release 12.4(11)T and later the default for this command is set to **infinity** for SCCP-controlled analog ports to prevent this timeout from expiring before the ringing no-answer timeout that is configured on Cisco Unified CallManager Express with the **timeouts ringing** command in telephony-service mode.

Examples

The following example configures voice port 0/0/1 to allow ringing for 600 seconds:

```
voice-port 0/0/1
 timeouts ringing 600
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a voice port.
timeouts interdigit	Configures the interdigit timeout value for a voice port.
timeouts ringing (telephony-service)	Sets the timeout value for ringing in a Cisco Unified CallManager Express system.

timeouts wait-release

To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts wait-release {*seconds* | **infinity**}

no timeouts wait-release

Syntax Description

seconds	Duration, in seconds, for which a voice port stays in the call-failure state while the Cisco router or concentrator sends a busy tone, reorder tone, or out-of-service tone to the port. Range is 3 to 3600. Default is 30.
infinity	The voice port is never released as long as the call-failure state remains.

Command Default

30 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1) MA	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to limit the time a voice port can be held in a call failure state. After the timeout, the release sequence is enabled.

You can also use this command for voice ports with Foreign Exchange Station (FXS) loop-start signaling to specify the time allowed for a caller to hang up before the voice port goes into the parked state.

Examples

The following example configures voice port 0/0/1 to stay in the call-failure state for 180 seconds while a busy tone, reorder tone, or out-of-service tone is sent to the voice port:

```
voice-port 0/0/1
 timeouts wait-release 180
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a voice port.
timeouts interdigit	Configures the interdigit timeout value for a voice port.

timeouts teardown lmr

To configure the time for which a Land Mobile Radio (LMR) voice port waits before tearing down an LMR connection after detecting no voice activity, use the **timeouts teardown lmr** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts teardown lmr {*seconds* | **infinity**}

no timeouts teardown lmr {*seconds* | **infinity**}

Syntax Description

seconds	Duration in seconds for which an LMR voice port waits before tearing down an LMR connection after detecting no voice activity. Valid values are 5 to 60000. The default is 180 seconds.
infinity	Disables disconnect supervision. The voice port does not disconnect when no voice activity is detected.

Command Default

180 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timeouts teardown lmr** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR.

Examples

The following example configures voice port 1/0/1 on a Cisco 3745 to remain connected for 6 seconds after no voice activity is detected by the voice port:

```
voice-port 1/0/1
 timeouts teardown lmr 6
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Specifies the delay time for releasing the calling voice port after a disconnect tone is received from the called voice port.
timeouts delay-duration	Configures the delay dial signal duration for a specified voice port.

timer accessrequest sequential delay

To configure the intermessage delay used when a border element (BE) is trying to determine a route from a list of neighboring BEs, use the **timer accessrequest sequential delay** command in Annex G configuration mode. To reset the default value, use the **no** form of this command.

timer accessrequest sequential delay *value*

no timer

Syntax Description

value	Amount of allowed intermessage delay (in increments of 100 ms). Range is from 0 to 10. The default is 1 (100 ms).

Command Default 1 (100 ms)

Command Modes Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines Setting the value of the delay to 0 causes the BE to broadcast or "blast" the AccessRequest messages to all eligible neighbors.

Examples The following example shows a timer delay of 1000 ms.

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# timer accessrequest sequential delay 10
```

Related Commands

Command	Description
call-router	Enables the Annex G border element configuration commands.

timer cluster-element

To configure the length of time between dynamic capacity messages to the local gatekeeper, use the **timer cluster-element** command in gatekeeper configuration mode. To stop sending dynamic updates, use the **no** form of this command.

timer cluster-element {**announce** | **resource-update**} *seconds*

no timer cluster-element

Syntax Description

announce	Configures the lengh of time between announcement messages to the gatekeepers in the local cluster.
resource-update	Configures the lengh of time between resource update messages to gatekeepers in the local cluster.
seconds	Number of seconds between resource updates sent to the gatekeeper. The valid range is 1 to 60. There is no default value.

Command Default

Disabled by default.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.4(11)T	The **resource-update** keyword was introduced.

Usage Guidelines

Use the **timer cluster-element** command to manage the length of time between resource updates and time between announcement messages sent to the gatekeeper. The announcement indication is exchanged at a set interval of time and carries information about the call and endpoint capacity for the zone. This allows the alternate gatekeepers to manage the bandwidth for a single zone even though the gatekeepers are in separate physical devices.

The gatekeeper assumes that the alternate gatekeeper has failed (and assumes that any previously allocated bandwidth is now available) if the gatekeeper does not receive an announcement message within six announcement periods or if the TCP connection with the gatekeeper is detected to be broken.

Lower this interval for closer tracking between elements. Raise it to lower messaging overhead.

Examples

The following command sets the announcement period to 20 seconds:

```
Router(config-gk)# timer cluster-element announce 20
```

The following command resets the announcement period to the default value:

```
Router(config-gk)# no timer cluster-element announce
```

The following example shows the time between resource update messages to gatekeepers in local cluster being set to 20 seconds:

```
Router(config-gk)# timer cluster-element resource-update 20
```

Related Commands

Command	Description
call-routing hunt-scheme	Enables capacity-based load-balancing.
zone cluster local	Defines a local grouping of gatekeepers.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

timer irr period

To configure the information request response (IRR) timer, or the periodic interval of IRR messages sent by the gatekeeper, use the **timer irr period** command in gatekeeper configuration mode. To disable, use the **no** form of this command.

timer irr period *minutes*

no timer irr period

Syntax Description

minutes	Length, in minutes, of the interval between IRR messages. Range is from 1 to 60. The default is 4.

Command Default 4 minutes

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use this command to configure IRR frequency that is included in the admission confirm (ACF) message. The IRR frequency is set to 240 seconds (4 minutes), based on an average 4-minute call hold time. The IRR allows the gatekeepers to terminate calls for which a disengage request (DRQ) has not been received. If missing DRQs are not a problem, the IRR frequency can be set to a larger value than 4 minutes, minimizing the number of unnecessary IRRs sent by a gateway.

Examples The following example shows that the IRR timer has been configured with a value of 45, meaning that IRR messages are sent by the gatekeeper every 45 minutes:

```
gatekeeper
.
.
.
lrq reject-resource-low
 no irq global-request
 timer lrq seq delay 10
 timer lrq window 6
 timer irr period 45
 no shutdown
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive LRQ messages.
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

timer lrq seq delay

To define the time interval between successive sequential location requests (LRQs), use the **timer lrq seq delay** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq seq delay *time*

no timer lrq seq delay

Syntax Description

time	Time interval, in 100-millisecond units. Range is 1 to 10 (0.1 to 1 second). The default is 5 (500 milliseconds).

Command Default 5 units (500 milliseconds)

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines The LRQ sequential timing source (SEQ) delay is used to set the time between sending LRQs to remote gatekeepers for address resolution. To resolve an address, the gatekeeper might have several remote zones configured, and it can send the LRQs simultaneously (blast) or sequentially (seq). The gatekeeper chooses the best route based on availability and cost. Using LRQs sequentially results in lower network traffic, but it can increase latency of calls when the most preferred route is unavailable.

Lowering the time increases traffic on the network but might reduce the call setup time.

Examples The following command sets the LRQ delay timer to 100 milliseconds:

```
timer lrq seq delay 1
```

The following command resets the LRQ delay timer to the default value:

```
no timer lrq seq delay
```

Related Commands

Command	Description
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.

timer lrq seq delay centisec

To define the time interval between successive sequential location requests (LRQs), use the **timer lrq seq delay centices** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq seq delay centisec *time*

no timer lrq seq delay centisec

Syntax Description

time	Time interval, in 100-millisecond units. Range is 1 to 10 (0.1 to 1 second). The default is 1(100 milliseconds).

Command Default

Timers are set to their default value.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The LRQ sequential timing source (SEQ) delay is used to set the time between sending LRQs to remote gatekeepers for address resolution. To resolve an address, the gatekeeper might have several remote zones configured, and it can send the LRQs simultaneously (blast) or sequentially (seq). The gatekeeper chooses the best route based on availability and cost. Using LRQs sequentially results in lower network traffic, but it can increase latency of calls when the most preferred route is unavailable.

Lowering the time increases traffic on the network but might reduce the call setup time.

Note This command cannot be configured at the same time as the **timer lrq seq delay** command.

Examples

The following command sets the LRQ delay timer to 100 milliseconds:

```
timer lrq seq delay centisec 1
```

The following command resets the LRQ delay timer to the default value:

```
no timer lrq seq delay centisec
```

Related Commands

Command	Description
timer lrq window decisec	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.

timer lrq window

To define the time window during which the gatekeeper collects responses to one or more outstanding LRQs, use the **timer lrq window** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq window *seconds*

no timer lrq window

Syntax Description

seconds	Time window, in seconds. Range is 1 to 15. The default is 3.

Command Default 3 seconds

Command Modes Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines Increasing the time can increase the call success rate but might reduce the overall time for call setup.

Examples The following command sets the timer to 5 seconds:

```
timer lrq window 5
```

The following command sets the timer to the default value:

```
no timer lrq window
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive sequential LRQs.

timer lrq window decisec

To define the time window during which the gatekeeper collects responses to one or more outstanding LRQs, use the **timer lrq window decisec** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq window decisec *time*

no timer lrq window decisec

Syntax Description

time	Time window, in seconds. Range is 1 to 15. The default is 2.

Command Default

Timers are set to their default value.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Increasing the time can increase the call success rate but might reduce the overall time for call setup.

Note This command cannot be in effect at the same time as the **timer lrq window** command.

Examples

The following command sets the timer to 5 seconds:

```
timer lrq window decisec 2
```

The following command sets the timer to the default value:

```
no timer lrq window decisec
```

Related Commands

Command	Description
timer lrq seq delay centsec	Defines the time interval between successive sequential LRQs.

timer media-inactive

To enable the timer for media inactivity detection using the digital signal processor (DSP) (based on RTP as the only criterion) and to configure a multiplication factor based on the real-time control protocol (RTCP) timer interval, use the **timer media-inactive** command in gateway configuration mode. To reset to the default, use the **no** form of this command.

timer media-inactive *multiple*

no timer media-inactive *multiple*

Syntax Description

multiple	Multiples of the RTCP report transmission interval. Range is 4 to 1000. The default is 5, and the recommended value is 5.

Command Default

A call is considered inactive if no RTP packet activity is detected for a period of time calculated as five times the interval set by the **ip rtcp report interval** command.

Command Modes

Gateway configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

When the **timer media-inactive** command is used, the gateway uses the inactivity timer as a combination of the **timer media-inactive** command and the **ip rtcp report interval** command. The **timer media-inactive** command uses DSP statistics. This capability is based on the configuration of callfeature parameters using application command-line interface (CLI) to enable control.

The media are considered inactive only if there is no transfer of RTP packets in the send direction and no RTP packets in the receive direction. If RTP is present in either the send or receive direction, it is considered active. In this mode, DSP filters out any comfort noise packets, and the presence of any comfort noise packet is considered inactivity in either direction.

The *multiple* argument (or multiplication factor) is multiplied by the interval that is set using the **ip rtcp report interval** command. This command configures the average interval between successive RTCP report transmissions for a given voice session. For example, if the *value* argument is set to 25,000 milliseconds, an RTCP report is sent every 25 seconds, on average. If no RTP packets are received during the calculated interval, the call is disconnected. The gateway signals the disconnect to the VoIP network and the time-division multiplexing (TDM) network so that upstream and downstream devices can clear their resources.

Examples

The following example uses the **ip rtcp report interval** command to set the reporting interval to 5000 milliseconds, and then the **timer media-inactive** command to set the multiplication factor to 10. The result is that calls detected as inactive for 50 seconds (5,000 milliseconds times 10) will be disconnected.

```
Router(config)# ip rtcp report interval 5000
Router(config)# gateway
Router(config-gateway)# timer media-inactive 10
Router(config-gateway)# exit
```

Related Commands

Command	Description
ip rtcp report interval	Configures the minimum interval of RTCP report transmissions.

timer receive-rtcp

To enable the Real-Time Control Protocol (RTCP) timer and to configure a multiplication factor for the RTCP timer interval for Session Initiation Protocol (SIP) or H.323, use the **timer receive-rtcp** command in gateway configuration mode. To reset to the default, use the **no** form of this command.

timer receive-rtcp *timer*

no timer receive-rtcp *timer*

Syntax Description

timer	Multiples of the RTCP report transmission interval. Range is 0 to 1000. Default is 0. Recommended value is 5.

Command Default

The default value for the *timer* argument is 0 multiples, which disables the timer so that no silence detection is in effect.

Command Modes

Gateway configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

The **timer receive-rtcp** command uses library-based detection and the receipt of either Real-Time Protocol (RTP) or RTCP packets is considered activity on a call. Silence detection occurs only if there are no packets received for both RTP and RTCP.

When the **ip rtcp report interval** and **timer receive-rtcp** commands are used, the gateway uses RTCP report detection, rather than RTP packet detection, to determine whether calls on the gateway are still active or should be disconnected. RTCP report detection is therefore more reliable than RTP packet detection because there can be periods during voice calls when one or both parties are not sending RTP packets.

One common example of a voice session in which no RTP is sent is when a caller dials into a conference call and mutes that endpoint. If voice activity detection (VAD, also known as silence suppression) is enabled, no RTP packets are sent while the endpoint is muted. However, the muted endpoint continues to send RTCP reports at the interval specified by the **ip rtcp report interval** command.

The **timer receive-rtcp** *timer* argument (or *m* factor for multiplication factor) is multiplied by the interval that is set using the **ip rtcp report interval** command. If no RTP or RTCP packets are received during the calculated interval, the call is disconnected. The gateway signals the disconnect to the VoIP network and the time-division multiplex (TDM) network so that upstream and downstream devices can clear their resources. The gateway sends a Q.931 DISCONNECT message to the TDM network and a

SIP BYE or H.323 ReleaseComplete message to the VoIP network to clear the call when the timer expires. The Q.931 DISCONNECT message is sent with a cause code value of 3 (no route) for SIP calls and a cause code value of 41 (temporary failure) for H.323 calls. No Q.931 Progress Indicator (PI) value is included in the DISCONNECT message.

To show timer-related output for SIP calls, use the **debug ccsip events** command. To show timer-related output for H.323 calls, use the **debug cch323 h225** command.

Examples

The following example sets the multiplication factor to 10 (or *x* * 10, where *x* is the interval that is set with the **ip rtcp report interval** command):

```
Router(config)# gateway
Router(config-gateway)# timer receive-rtcp 10
Router(config-gateway)# exit
```

Related Commands

Command	Description
debug cch323 h225	Traces the state transition of the gateway H.225 state machine based on the processed events.
debug ccsip events	Displays all SIP SPI events tracing and traces the events posted to SIP SPI from all interfaces.
ip rtcp report interval	Configures the minimum interval of RTCP report transmissions.

timer receive-rtp

To configure the Real-Time Transport Protocol (RTP) timeout interval to clear connections that pause indefinitely, use the **timer receive-rtp** command in gateway configuration mode. To reset the timer to the default value, use the **no** form of this command.

timer receive-rtp *seconds*

no timer receive-rtp

Syntax Description

seconds	Timer value, in seconds. Range: 180 to 86400. Default: 1200.

Defaults

1200 seconds (20 minutes)

Command Modes

Gateway configuration (config-gateway)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(20)T	This command was modified. The recommended timer range is defined as 1200 seconds.

Usage Guidelines

This command is used to configure the RTP timeout interval in seconds. The timeout value is used to clear connections that pause indefinitely. The recommended value is 1200 seconds, or 20 minutes.

Examples

The following example shows the RTP timeout interval set to the recommended 1200 seconds (20 minutes).

```
Router(config-gateway)# timer receive-rtp 600
```

Related Commands

Command	Description
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.

timer server retry

To set the gatekeeper's retry timer for failed Gatekeeper Transaction Message Protocol (GKTMP) connections, use the **timer server retry** command in gatekeeper configuration mode. To reset the timer to its default, use the **no** form of this command or the **default server timer retry** command.

server timer retry *seconds*

no server timer retry

default server timer retry

Syntax Description

seconds	Number of seconds for which the gatekeeper should wait before retrying the GKTMP server. Range is from 1 through 300. The default is 30.

Command Default

30 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

After the gatekeeper detects that its GKTMP server TCP connection has failed, the gatekeeper retries the server after an interval based on the setting of this timer, and keeps retrying until the connection is established.

This timer applies only to deployments where static triggers are used between the gatekeeper and the GKTMP server. If dynamic triggers are used, the server must determine and implement a retry mechanism if the TCP connection to the gatekeeper fails.

Examples

The following example shows that the retry timer has been set to 45 seconds:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 timer server retry 45
 no shutdown
.
.
.
```

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

timer server timeout

To specify the timeout interval for a response from a back-end Gatekeeper Transaction Message Protocol (GKTMP) application server, use the **timer server timeout** command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer server timeout *time*

no timer server timeout

Syntax Description

time	Timeout interval, in 100-ms units. Range is 1 to 50 (0.1 to 5 seconds). Default is 3 (300 ms).

Command Default

3 units

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

Use this command to specify the timeout interval for a response from a back-end GKTMP application server.

Examples

The following command sets the timeout interval to 400 ms:

```
timer server timeout 4
```

The following command resets the timeout interval to the default value:

```
no timer server timeout
```

Related Commands

Command	Description
server registration-port	Configures the listener port for the server to establish a connection with the gatekeeper.
server trigger	Configures a static server trigger for external applications.

timers

To configure the Session Initiation Protocol (SIP) signaling timers, use the **timers** command in SIP UA configuration mode. To restore the default value, use the **no** form of this command.

timers {**trying** *number* | **connect** *number* | **disconnect** *number* | **expires** *number*}

no timers

Syntax Description

trying *number*	Time (in milliseconds) to wait for a 100 response to an INVITE request. Range is from 100 to 1000. The default is 500.
connect *number*	Time (in milliseconds) to wait for a 200 response to an ACK request. Range is from 100 to 1000. The default is 500.
disconnect *number*	Time (in milliseconds) to wait for a 200 response to a BYE request. Range is from 100 to 1000. The default is 500.
expires *number*	Time (in milliseconds) for which an INVITE request is valid. Range is from 60000 to 300000. The default is 180000.

Command Default

trying, **connect**, and **disconnect**—500 ms
expires—180000 ms

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (**invite-wait-180** and **invite-wait-200**) were combined into one (**trying**).
12.2(2)XA	This command was implemented on the Cisco AS5400 and AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you used an earlier version of this command to configure timers, the timer settings are maintained. The output of the **show running-config** command reflects both previous and current timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets the trying timers to the default of 500 ms.

```
Router(config)# sip-ua
Router(config-sip-ua)# timers trying 500
```

Related Commands

Command	Description
default	Sets a command to its default.
inband-alerting	Specifies an inband-alerting SIP header.
max-forwards	Specifies the maximum number of hops for a request.
retry (SIP UA)	Configures the SIP signaling timers for retry attempts.
transport	Enables SIP UA transport for TCP/UDP.

timers buffer-invite

To enable the Session Initiation Protocol (SIP) buffer-invite timer and to configure the timer interval, use the **timers buffer-invite** command in SIP UA configuration mode. To restore the default value, use the **no** form of this command.

timers buffer-invite *timer*

no timers buffer-invite

Syntax Description

timer	Buffer-invite timer value, in ms. Range is 50 to 5000.

Command Default Disabled

Command Modes SIP UA configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines Use this command to enable the SIP buffer-invite timer and to configure the timer interval.

Examples The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers buffer-invite 500
```

Related Commands

Command	Description
sip-ua	Enables SIP UA configuration commands.

timers comet

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting conditions-met (COMET) requests, use the **timers comet** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers comet *time*

no timers comet

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

COMET, or conditions met, indicates whether preconditions for a given call or session have been met. This command is applicable only with calls involving quality of service (QoS) (calls other than best-effort).

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers comet 500
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
timers prack	Sets how long the UA waits before retransmitting a PRACK request.

timers connect

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits for a 200 response to an ACK request, use the **timers connect** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers connect *number*

no timers connect *number*

Syntax Description

number	Waiting time, in milliseconds. Range is from 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the **show running-config** command reflects both timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets connect time to 200 milliseconds:

```
sip-ua
 timers connect 200
```

Related Commands

Command	Description
sip-ua	Enables the SIP UA configuration commands.

timers connection aging

To globally set the time before the Session Initiation Protocol (SIP) user agent (UA) ages out a TCP or UDP connection because of inactivity, use the **timers connection aging** command in SIP UA configuration mode. To reset this time to the default value, use the **no** form of this command.

timers connection aging *timer-value*

no timers connection aging

Syntax Description

timer-value	Time to wait, in minutes, before aging out a TCP or UDP connection because of inactivity. Range is from 5 to 30. Default is 5.

Command Default

5 minutes

Command Modes

SIP UA configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The minimum value of this connection is 5 minutes.

Examples

The following example ages out a connection in 10 minutes:

```
sip-ua
 timers connection aging 10
```

Related Commands

Command	Description
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP UA configuration commands.
timers expires	Sets how long a SIP INVITE request is valid.

timers disconnect

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits for a 200 response to a BYE request, use the **timers disconnect** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers disconnect *time*

no timers disconnect *time*

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS400.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series. Supported for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the **show running-config** command reflects both timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets disconnect time to 200 milliseconds:

```
sip-ua
 timers disconnect 200
```

Related Commands

Command	Description
sip-ua	Enables the SIP UA configuration commands.

timers expires

To set how long a Session Initiation Protocol (SIP) INVITE request is valid, use the **timers expire** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers expires *time*

no timers expires

Syntax Description

time	Expiration time, in ms. Range is 60,000 to 300,000. Default is 180000.

Command Default

180000 ms

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the **show running-config** command reflects both timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets the expiration time to 180,000 ms:

```
sip-ua
 timers expires 180000
```

Related Commands

Command	Description
default	Enables a default aggregation cache.

Command	Description
sip-ua	Enables the SIP UA configuration commands.
timers	Configures the SIP signaling timers.

timers hold

To enable the Session Initiation Protocol (SIP) hold timer and configure the timer interval before disconnecting a held call, use the **timers hold** command in SIP UA configuration mode. To restore the default value, use the **no** form of this command.

timers hold *time*

no timers hold

Syntax Description

time	Specifies the time (in minutes) to wait before sending a BYE request. Range is from 15 to 2880 minutes. The default is 2880.

Command Default

Enabled

time: 2880 minutes

Command Modes

SIP UA configuration mode

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The hold timer is typically activated when a gateway receives a call hold request from the other endpoint, for example, a SIP phone.

Examples

The following example sets the hold timer to expire after 75 minutes:

```
Router(config-sip-ua)# timers hold 75
```

Related Commands

Command	Description
show sip-ua timers	Displays the current settings for SIP user agent timers.
suspend-resume	Enables SIP Suspend and Resume (call-hold) functionality.
timer receive-rtcp	Enables media inactivity Real-Time Control Protocol (RTCP) timer.

timers keepalive

To set the keepalive timers interval between sending Options message requests when the session initiation protocol (SIP) servers are in the down state, use the **timers keepalive** command in SIP user agent configuration mode. To restore the keepalive timers to the default value of 120 seconds when active or 30 seconds when down, use the **no** form of this command.

timers keepalive {**active** | **down**} *seconds*

no timers keepalive {**active** | **down**} *seconds*

Syntax Description

active	SIP servers are in the active state.
down	SIP servers are in the down state.
seconds	Time in seconds between keepalive messages when the SIP servers are either active or down, as follows: • If **active** is specified, the range is from 10 to 600 seconds; the default value is 120 seconds. • If **down** is specified, the range is from 1 to 120 seconds; the default value is 30 seconds.

Command Default

The default value for the active state is 120 seconds and the default value for the down state is 30 seconds.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command to change the keepalive message time interval in seconds between the sending Options message requests when the SIP server or servers are either in the active or down state.

Examples

The following example sets the keepalive message time interval to 20 seconds when the SIP server is in the active state:

```
sip-ua
 timers keepalive active 20
```

The following example sets the keepalive message time interval to 10 seconds when the SIP server is in the down state:

```
sip-ua
 timers keepalive down 10
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
keepalive trigger	Sets the time interval to the number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
retry keepalive	Sets the retry keepalive interval for retransmission.

timers notify

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a Notify message, use the **timers notify** command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

timers notify *time*

no timers notify

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Defaults

500 milliseconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

A Notify message informs the user agent that initiated the transfer or Refer request about the outcome of the SIP transaction.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers notify 500
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, timer, and retry statistics
show sip-ua timers	Displays the current settings for SIP UA timers

timers prack

To set how long the Session Initiation Protocol (SIP) user agent (UA) wait s before retransmitting a provisional response acknowledgement (PRACK) request, use the **timers prack** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers prack *time*

no timers prack

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

PRACK allows reliable exchanges of SIP provisional responses between SIP endpoints. When the retransmission value is set, retransmissions are sent with an exponential backoff of up to 4 seconds. That is, the retransmission interval for each packet increases exponentially until 4 seconds is reached.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers prack 500
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
timers comet	Sets how long the UA waits before retransmitting a COMET request.

timers refer

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a Refer request, use the **timers refer** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers refer *time*

no timers refer

Syntax Description

time	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Usage Guidelines

A SIP Refer request is sent by the originating gateway to the receiving gateway and initiates call forward and call transfer capabilities.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers refer 500
```

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.

timers register

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before sending register requests, use the **timers register** command in SIP user-agent configuration mode. To reset this value to the default, use the **no** form of this command.

timers register *milliseconds*

no timers register

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Defaults

500 milliseconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	Support for IPv6 was added.

Examples

The following example sends register requests every 500 milliseconds:

```
sip-ua
 retry invite 9
 retry register 9
 timers register 500
```

Related Commands

Command	Description
retry register	Sets the total number of SIP registers to send.

timers rel1xx

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a reliable1xx response, use the **timers rel1xx** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers rel1xx *time*

no timers rel1xx

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was inplemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Examples

The following example sets retransmission time to 400 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers rel1xx 400
```

Related Commands

Command	Description
retry rel1xx	Configures how many times the reliable1xx response is retransmitted.
show sip-ua statistics	Displays response, traffic, timer, and retry statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.

timers trying

To set how long the Session Initiation Protocol (SIP) user agent (UA) wait s for a 100 response to a SIP INVITE request, use the **timers trying** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

timers trying *time*

no timers trying

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP UA configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the **show running-config** command reflects both timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets trying time to 500 milliseconds.

```
sip-ua
 timers trying 500
```

Related Commands

Command	Description
sip-ua	Enables the SIP UA configuration commands.

timing clear-wait

To set the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port, use the **timing clear-wait** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing clear-wait *time*

no timing clear-wait

Syntax Description

time	Minimum time, in milliseconds, between an inactive seizure signal and the call being cleared. Cisco 3600 series range is from 200 to 2000. The default for both is 400.

Command Default 400 milliseconds

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 2600 and Cisco 3600 series routers.

Usage Guidelines This command is supported on E&M ports only.

Examples The following example sets the clear-wait duration on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing clear-wait 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-duration

To specify the delay signal duration for a specified voice port, use the **timing delay-duration** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-duration *time*

no timing delay-duration *time*

Syntax Description

time	Delay signal duration for delay dial signaling, in milliseconds. Range is from 100 to 5000. The default is 2000.

Command Default

2000 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

The call direction for the **timing delay-duration** command is out. This command is supported on E&M ports only.

Examples

The following example sets the delay signal duration on a voice port to 3000 milliseconds:

```
voice-port 1/0/0
 timing delay-duration 3000
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-start

To specify the minimum delay time from outgoing seizure to out-dial address for a specified voice port, use the **timing delay-start** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-start *time*

no timing delay-start

Syntax Description

time	Minimum delay time, in milliseconds, from outgoing seizure to outdial address. Range is from 20 to 2000. The default on the Cisco 3600 series is 300.

Command Default

Cisco 3600 series: 300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

The call direction for the **timing delay-start** command is out. It is supported on E&M ports only.

Examples

The following example sets the delay-start duration on a voice port to 250 milliseconds:

```
voice-port 1/0/0
 timing delay-start 250
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.

Command	Description
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-voice tdm

To specify the delay after which voice packets are played out, use the **timing delay-voice tdm** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-voice tdm *milliseconds*

no timing delay-voice tdm *milliseconds*

Syntax Description

milliseconds	Duration, in milliseconds, of the timing delay. Range is integers from 1 to 1500. Default is 0.

Command Default

milliseconds: 0 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

The **timing delay-voice tdm** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). To avoid voice loss at the receiving end of an LMR system, use this command to configure a delay for the voice packet equal to the sum of the durations of all the injected tones and pauses configured with the **inject tone** command and the **inject pause** command.

Examples

The following example configures a timing delay of 470 milliseconds before the voice packet is played out:

```
voice class tone-signal mytones
 inject tone 1 1950 3 150
 inject tone 2 2000 0 60
 inject pause 3 60
 inject tone 4 2175 3 150
 inject tone 5 1000 0 50
voice-port 1/0/0
 voice-class tone-signal mytones
 timing delay-voice tdm 470
```

Note that the delay of 470 milliseconds is equal to the sum of the durations of the injected tones and pauses in the tone-signal voice class.

Related Commands

Command	Description
inject pause	Specifies a pause between injected tones.
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.

timing delay-with-integrity

To specify the duration of the wink pulse for the delay dial for a specified voice port, use the **timing delay-with-integrity** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-with-integrity *time*

no timing delay-with-integrity

Syntax Description

time	Duration of the wink pulse for the delay dial, in milliseconds. Range is from 0 to 5000. The default is 0.

Command Default 0 milliseconds

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines This command is supported on E&M ports only.

Examples The following example sets the duration of the wink pulse for the delay dial to 10 milliseconds:

```
voice-port 1/0/0
 timing delay-with-integrity 10
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.

Command	Description
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing dialout-delay

To specify the dial-out delay for the sending digit on a specified voice port, use the **timing dialout-delay** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing dialout-delay *time*

no timing dialout-delay *time*

Syntax Description

time	Dial-out delay, in milliseconds, for the sending digit or cut-through on a Foreign Exchange Office (FXO) trunk or an E&M immediate trunk. Range is from 100 to 5000. The default is 300.

Command Default

300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.

Examples

The following example sets the dial-out delay to 350 milliseconds:

```
voice-port 1/0/0
 timing dialout-delay 350
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.

Command	Description
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing dial-pulse min-delay

To specify the time between wink-like pulses for a specified voice port, use the **timing dial-pulse min-delay** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing dial-pulse min-delay *time*

no timing dial-pulse min-delay

Syntax Description

time	Time between wink-like pulses, in milliseconds. Range is from 0 to 5000. The default is 300.

Command Default

300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

Use the **timing dial-pulse min-delay** command with PBXs that require a wink-like pulse, even though they have been configured for delay-dial signaling. If the value for this argument is set to 0, the router does not generate this wink-like pulse. The call signal direction for this command is in.

Examples

The following example sets the time between the generation of wink-like pulses on a voice port to 350 milliseconds:

```
voice-port 1/0/0
 timing dial-pulse min-delay 350
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.

Command	Description
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing digit

To specify the dual tone multifrequency (DTMF) digit signal duration for a specified voice port, use the **timing digit** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing digit *time*

no timing digit

Syntax Description

time	The DTMF digit signal duration, in milliseconds. Range is 5 from 0 to 100. The default is 100.

Command Default

100 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

The call signal direction for the **timing digit** command is out. This command is supported on Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and E&M ports.

Examples

The following example sets the DTMF digit signal duration on a voice port to 50 milliseconds:

```
voice-port 1/0/0
 timing digit 50
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.

Command	Description
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing guard-out

To specify the guard-out duration of a Foreign Exchange Office (FXO) voice port, use the **timing guard-out** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing guard-out *time*

no timing guard-out

Syntax Description

time	Duration of the guard-out period, in milliseconds. The range is from 300 to 3000. The default is 2000.

Defaults

The default is 2000 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command is supported on FXO voice ports only.

For Caller ID to work for FXO ports registered to a Cisco Unified CM, the range in milliseconds must be between 1000 to 2000.

Examples

The following example sets the timing guard-out duration on a voice port to 1000 milliseconds:

```
voice-port 1/0/0
 timing guard-out 1000
```

timing hangover

To specify the number of milliseconds of delay before the digital signal processor (DSP) tells Cisco IOS software to turn off the E-lead after the DSP detects that the voice stream has stopped, use the **timing hangover** command in voice-port configuration mode. To return to the default value, use the **no** form of this command.

timing hangover *milliseconds*

no timing hangover *milliseconds*

Syntax Description

milliseconds	The number of milliseconds for which the E-lead stays active after VAD determines that the voice stream has stopped. Valid values are 0 to 10000. The default is 250 milliseconds.

Command Default

milliseconds: 250 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timing hangover** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). If the voice port has been configured with the **lmr e-lead voice** command, use the **timing hangover** command to adjust the timing if the E-lead is being turned on and off too frequently.

Examples

The following example configures E-lead on voice port 1/0/1 on a Cisco 3745 to stay active for 300 milliseconds after VAD determines that the voice stream has stopped:

```
voice-port 1/0/1
 timing hangover 300
```

timing hookflash-input

To specify the maximum duration of an on-hook condition that will be interpreted as a hookflash by the Cisco IOS software, use the **timing hookflash-input** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-input *milliseconds*

no timing hookflash-input

Syntax Description

milliseconds	Upper limit of the hookflash duration range, in milliseconds. • E&M voice ports—Range is 0 to 1550 milliseconds. Default is 480 milliseconds. • FXS voice ports—Range is 50 to 1550 milliseconds. Default is 1000 milliseconds.

Command Default

milliseconds: 480 milliseconds for E&M voice ports, 1000 milliseconds for FXS voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 3600 series.
12.3(7)T	Lower limit of the range for E&M voice ports was extended to 0 milliseconds.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

This command is applied to E&M or Foreign Exchange Station (FXS) interfaces.

For Land Mobile Radio E&M voice ports, the **timing hookflash-input** command configures the delay between when the M-lead is raised and when voice is transmitted. Setting the hookflash duration to 0 milliseconds specifies no delay in the audio input and eliminates front-end clipping.

Analog phones connected to FXS ports use hookflash to access a second dial tone to initiate some phone features, such as transfer and conference. Hookflash is an on-hook condition of short duration that is usually generated when a phone user presses the Flash button on a phone. Cisco voice gateways measure the duration of detected on-hook conditions to determine whether they should be interpreted as hookflash or not. The duration for the on-hook conditions generated by Flash buttons on phones varies for different phone types and is interpreted by Cisco IOS software as follows:

- An on-hook condition that lasts for a time period that falls inside the hookflash duration range is considered a hookflash.
- An on-hook condition that lasts for a shorter period than the lower limit of the range is ignored.
- An on-hook condition that lasts for a longer period than the higher limit of the range is considered a disconnect.

The hookflash duration range for FXS voice ports is defined as follows:

- The lower limit of the range is set in software at 150 ms, although there is also a hardware-imposed lower limit that is typically about 20 ms, depending on platform type. An on-hook condition that lasts for a shorter time than this hardware-imposed lower limit is simply not reported to the Cisco IOS software.
- The upper limit of the range is set in software at 1000 ms by default, although this value can be changed using the **timing hookflash-input** command in voice-port configuration mode on the voice gateway. The upper limit can be set to any value from 50 to 1550 ms. For more information, see the explanations in the "Examples" section.

This command does not affect whether hookflash relay is enabled; hookflash relay is enabled only when the **dtmf-relay h245-signal** command is configured on the applicable VoIP dial peers. When the **dtmf-relay h245-signal** command is configured, the H.323 gateway relays hookflash by using an H.245 "signal" User Input Indication method. Hookflash is sent only when an H.245 signal is available.

Examples

The following example sets an upper limit of 200 milliseconds for the hookflash duration range:

```
voice-port 1/0/0
 timing hookflash-input 200
```

If the **timing hookflash-input** command is set to X, a value greater than 150, then any on-hook duration between 150 and X is interpreted as a hookflash. For example, if X is 1550, the hookflash duration range is 150 to 1550 ms. An on-hook signal that lasts for 1250 ms is interpreted as a hookflash, but an on-hook signal of 55 ms is ignored.

```
voice-port 1/0/0
 timing hookflash-input 1550
```

If the **timing hookflash-input** command is set to X, a value less than 150, then any on-hook duration between Y, the hardware lower limit, and X is interpreted as a hookflash. For example, if X is 65, the hookflash duration range is Y to 65 ms. An on-hook signal that lasts for 1250 ms is interpreted as a disconnect, but an on-hook signal of 55 ms is interpreted as a hookflash. (This example assumes that Y for the voice gateway is lower than 55 ms.)

```
voice-port 1/0/0
 timing hookflash-input 65
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.

timing hookflash-output

To specify the duration of hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface, use the **timing hookflash-output** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-output *time*

no timing hookflash-output

Syntax Description

time	Duration of the hookflash, in milliseconds. Range is from 50 to 1550. The default is 400 milliseconds.

Command Default 400 milliseconds

Command Modes Voice-port configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2500, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines This command does *not* affect whether hookflash relay is enabled; hookflash relay is enabled only when the **dtmf-relay h245-signal** command is configured on the applicable VoIP dial peers. Hookflash is relayed by using an H.245-signal indication and can be sent only when an H.245 signal is available.

Use the **timing hookflash-output** command on FXO interfaces to specify the duration (in milliseconds) of a hookflash indication. To set hookflash timing parameters for analog voice interfaces, use the **timing** command.

Examples The following example implements timing for the hookflash with a duration of 200 milliseconds.

```
voice-port 1/0/0
 timing hookflash-output 200
```

Related Commands

Command	Description

dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
voice-port	Enters voice-port configuration mode.

timing ignore m-lead

To ignore M-lead or voice activity detection (VAD) changes for a specified amount of time after sending the E-lead off signal, use the **timing ignore m-lead** command in voice-port configuration mode. To return to the default value, use the **no** form of this command.

timing ignore m-lead *milliseconds*

no timing ignore m-lead *milliseconds*

Syntax Description

milliseconds	The number of milliseconds following the sending of the E-lead off signal for which the M-lead and VAD changes are ignored. Valid values are 0 to 10000. The default is 0 milliseconds.

Command Default

milliseconds: 0 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

- The **timing ignore m-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Use this command to reduce echo feedback on an LMR voice port. This command has an effect only if the voice port is configured for half duplex mode.

Examples

The following example configures voice port 1/0/1 on a Cisco 3745 to ignore M-lead or VAD changes for 500 milliseconds after sending the E-lead off signal:

```
voice-port 1/0/1
 timing ignore m-lead 500
```

timing interdigit

To specify the dual-tone multifrequency (DTMF) interdigit duration for a specified voice port, use the **timing interdigit** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing interdigit *time*

no timing interdigit *time*

Syntax Description

time	DTMF interdigit duration, in milliseconds. Range is from 50 to 500. The default is 100.

Command Default

100 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing interdigit** command is out. This command is supported on Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and E&M ports.

Examples

The following example sets the DTMF interdigit duration on a voice port to 150 milliseconds:

```
voice-port 1/0/0
 timing interdigit 150
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.

Command	Description
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing opx-ringwait

To set the maximum wait time for detecting the next ring on FXO ports, use the **timing opx-ringwait** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing opx-ringwait *msecs*

no timing opx-ringwait

Syntax Description

msecs	Maximum duration, in milliseconds, to wait for the next ring. Range is 2000 to 10000. Default is 6000.

Command Default

Timeout for detecting ring tones is 6000 ms (6 sec).

Command Modes

Voice-port configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command prevents the voice gateway from prematurely disconnecting private line automatic ring-down (PLAR) off-premises extension (OPX) calls when the duration between ring tones from the switch is more than 6 sec. The absence of a ring tone from the switch indicates that the originating party has disconnected the call. Because some analog switches take longer than 6 sec to generate the ring tone, the voice gateway could clear the call leg while it is still ringing for a PLAR OPX call, unless the 6-sec default is changed with this command.

Examples

The following example sets the timeout for the next ring to 8 sec:

```
voice-port 2/0/10
 timing opx-ringwait 8000
```

Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.
show voice port	Displays configuration information about a specific voice port.

timing percentbreak

To specify the percentage of the break period for dialing pulses for a voice port, use the **timing percentbreak** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing percentbreak *percent*

no timing percentbreak

Syntax Description

percent	Percentage of the break period for dialing pulses. Range is from 20 to 80. The default is 50.

Command Default

50 percent

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA4	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **timing percentbreak** command is supported on Foreign Exchange Office (FXO) and E&M voice ports only.

Examples

The following example sets the break period percentage on a voice port to 30 percent:

```
voice-port 0/0/1
 timing percentbreak 30
```

Related Commands

Command	Description
timing pulse	Configures the pulse dialing rate for a voice port.
timing pulse-interdigit	Configures the pulse interdigit timing for a voice port.

timing pulse

To specify the pulse dialing rate for a specified voice port, use the **timing pulse** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing pulse *pulses-per-second*

no timing pulse *pulses-per-second*

Syntax Description

pulses-per-second	Pulse dialing rate, in pulses per second. Range is from 10 to 20. The default is 20.

Command Default

20 pulses per seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was supported on the Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing pulse** command is out. This command is supported on Foreign Exchange Office (FXO) and E&M ports only.

Examples

The following example sets the pulse dialing rate on a voice port to 15 pulses per second:

```
voice-port 1/0/0
 timing pulse 15
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing pulse-interdigit

To specify the pulse interdigit timing for a specified voice port, use the **timing pulse-interdigit** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing pulse-interdigit *time*

no timing pulse-interdigit *time*

Syntax Description

time	Pulse dialing interdigit timing, in milliseconds. Range is from 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing pulse-interdigit** command is out. This command is supported on Foreign Exchange Office (FXO) and E&M ports only.

Examples

The following example sets the pulse-dialing interdigit timing on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing pulse-interdigit 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.

Command	Description
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing sup-disconnect

To define the minimum time to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX), use the **timing sup-disconnect** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

timing sup-disconnect *milliseconds*

no timing sup-disconnect *milliseconds*

Syntax Description

milliseconds	Minimum time, in milliseconds, after detection of an on-hook indication to determine that the on-hook condition is intentional and then to hang up the POTS call leg. The range is from 50 to 1500. The default is 350.

Command Default

The default minimum time is 350 milliseconds before a supervisory disconnect occurs.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(12)	This command was introduced.
12.3(11)T6	This command was integrated into Cisco IOS Release 12.3(11)T6.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).

Usage Guidelines

Prior to the implementation of the **timing sup-disconnect** command, analog Foreign Exchange Office (FXO) ports could not detect short disconnect signals lasting fewer than 350 ms in duration. Using this command, you can specify a wait period from 50 to 1500 ms to ensure that when an on-hook indication persists for a time that is longer than the configured value, the on-hook condition is considered intentional and a hang-up is signaled on the POTS call leg.

This timer affects only analog loop-start FXO voice ports.

Even though the **timing sup-disconnect** command can be entered under the voice port in FXO ground-start signaling, the changes in the timer setting take effect only in FXO loop-start signaling.

Examples

The following example sets the timer to wait 500 ms after detecting an on-hook signal before a supervisory disconnect occurs on the POTS call leg:

```
voice-port 1/0/0
 timing sup-disconnect 500
```

Related Commands

Command	Description
show voice port	Displays configuration information about a specific voice port.
voice-port	Enters voice-port configuration mode.

timing wait-wink

To set the maximum time to wait for wink signal after an outgoing seizure is sent, use the **timing wait-wink** command in voice port configuration mode. To restore the default value, use the **no** form of this command.

timing wait-wink *milliseconds*

no timing wait-wink *milliseconds*

Syntax Description

milliseconds	Maximum time to wait for wink signal after an outgoing seizure is sent. Valid entries are from 100 to 6500 milliseconds (ms). Supported on ear and mouth (E&M) ports only.

Defaults

milliseconds: 550 milliseconds

Command Modes

Voice port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.
11.3(1)MA	This command was implemented on Cisco MC3810 multiservice concentrators.
12.4(12)	The millisecond range was extended from 5000 to 6500.

Examples

The following example configures the maximum time to wait for wink signaling after an outgoing seizure is sent on a voice port for 300 milliseconds:

```
voice-port 1/0/0
 timing wait-wink 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.

Command	Description
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dial-out delay for the sending digit on a specified voice port.
timing delay-with-integrity	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing wink-duration

To specify the timing for transmit and receive wink-signal duration for a voice port, use the **timing wink-duration** command in voice-port configuration mode. To reset to the default values, use the **no** form of this command.

timing wink-duration {*time* | **receive** *minimum maximum*}

no timing wink-duration

Syntax Description

time	Maximum transmit duration, in milliseconds (ms), for a wink-start signal. The range is from 50 to 3000. The default is 200.
receive	Indicates that a range is to be specified for a received wink-start signal.
minimum	Received minimum wink length, in milliseconds. The range is from 40 to 2950. The default is 140.
maximum	Received maximum wink length, in milliseconds. The range is from 150 to 3150. The default is 290.

Command Default

Transmit wink-duration timing is set to 200 ms. The received wink-duration timing minimum is set to 140 ms and the maximum is set to 290 ms.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was integrated into Cisco IOS Release 11.3(1)MA and support was added for the Cisco MC3810.
12.4(13)	This command was integrated into Cisco IOS Release 12.4(13) and the **receive** keyword and *minimum* and *maximum* arguments were added.

Usage Guidelines

The call signal direction for the **timing wink-duration** command is out. This command is supported on ear and mouth (E&M) ports only.

When wink-start signaling is used, the originating side seizes the line by going off-hook and then waits for an acknowledgment from the other end before initiating a call. The acknowledgment is a reversal of polarity (off-hook) for a timing period referred to as a wink. A wink should occur no earlier than 100 ms after the receipt of the incoming seizure signal. In addition to the signaling function, the wink start serves as an integrity check that identifies a malfunctioning trunk and allows the network to send a reorder tone to the calling party.

When you set the receive range, the minimum and maximum values of acceptable wink must provide an acceptable range of at least 50 ms. For example, entering the command **timing wink-duration receive 160 200** results in an error message.

Examples

The following example shows how to set the transmit wink-signal duration on voice port 1/0/0 to 300 ms:

```
voice-port 1/0/0
 timing wink-duration 300
```

The following example shows how to set the range for the receive wink-signal duration on voice port 1/0/0 to 160 to 210 ms:

```
voice-port 1/0/0
 timing wink-duration receive 160 210
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing delay-with-integrity	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing wink-wait

To specify the maximum wink-wait duration for a specified voice port, use the **timing wink-wait** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing wink-wait *time*

no timing wink-wait

Syntax Description

time	Maximum wink-wait duration, in milliseconds, for a wink start signal. Range is from 100 to 6500. The default is 200.

Defaults

200 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.
12.4(12)	The millisecond range was extended from 5000 to 6500.

Usage Guidelines

The call signal direction for the **timing wink-wait** command is out. This command is supported on ear and mouth (E&M) ports only.

Examples

The following example sets the wink-wait duration on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing wink-wait 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.

Command	Description
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.

tls

To enable Transport Layer Security (TLS) for the Skinny Client Control Protocol (SCCP) connection between the SCCP server and the SCCP client, use the **tls** command in DSP farm profile configuration mode. To disable secure SCCP signaling, use the **no** form of this command.

tls

no tls

Syntax Description

This command has no arguments or keywords.

Command Default

Secure SCCP signaling exchange is enabled by default.

Command Modes

DSP farm profile configuration (config-dspfarm-profile #)

Command History

Release	Modification
12.4(22)YB	This command was introduced.

Usage Guidelines

Use the **tls** command to enable secure SCCP signaling exchange. The configuration can be modified only when the dspfarm profile is shut down. To shut down the dsp farm profile, configure the **no shutdown** command.

Examples

The following example shows how to configure the **tls** command to enable TLS support for digital signal processor (DSP) farm services profile 1:

```
Router(config)# dspfarm profile 1 transcode security
Router(config-dspfarm-profile)# tls
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

toggle-between-two-calls

To define a Feature Access Code (FAC) to access the Toggle Between Two Calls feature in feature mode on analog phones connected to FXS ports, use the **toggle-between-two-calls** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

toggle-between-two-calls *keypad-character*

no toggle-between-two-calls

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0—9, *, #). Default is #5.

Command Default

The default value is #5.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for Toggle Between Two Calls from the default (#5) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Examples

The following example shows how to change the value of the feature code for the Toggle Between Two Calls feature from the default (#5). With this configuration, a phone user in basic call mode presses hook flash to get the first dial tone, then dials an extension number to connect to a second call. During the second call, the user presses a hook flash to get a feature tone and then dials 55 to toggle back to the previous call party.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# toggle-between-two-calls 55
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

token-root-name

To specify which root or Certificate Authority (CA) certificate the router uses to validate the settlement token in the incoming setup message, use the **token-root-name** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

token-root-name *name*

no token-root-name

Syntax Description

name	Certificate identification name as configured with the **crypto ca identity** *name* command or the **crypto ca trusted-root** *name* command.

Command Default

The terminating gateway uses the CA certificate to validate the settlement token.

Command Modes

Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, Cisco AS5300, and Cisco AS5800.

Examples

The following example defines the token-root-name as “sample”:

```
token-root-name sample
```

The following example shows new output for the **show settlement** command to display the value of the **token-root-name** command:

```
Settlement Provider 0
        Operation Status = UP
        Type = osp
        Address url = https://1.14.115.100:8444/
        Encryption = all                (default)
        Token Root Name = sample
        Max Concurrent Connections = 20 (default)
        Connection Timeout = 3600 (s)   (default)
        Response Timeout = 1 (s)        (default)
        Retry Delay = 2 (s)             (default)
        Retry Limit = 1                 (default)
        Session Timeout = 86400 (s)     (default)
        Customer Id = 1000
        Device Id = 2000
        Roaming = Disabled              (default)
        Signed Token = On

        Number of Connections = 1
        Number of Transactions = 0
```

Related Commands

Command	Description
crypto ca identity	Declares the Certificate Authority that your router should use.
crypto ca trusted-root	Configures the root certificate that the server uses to sign the settlement tokens.
show settlement	Displays the configuration for all settlement server transactions.

tone busytone

To enable automatic busytone generation in a basic call scenario, use the **tone busytone** command in dial peer voice configuration mode. To disable automatic busytone generation, use the **no** form of this command.

tone busytone remote-onhook

no tone busytone remote-onhook

Syntax Description

remote-onhook	Generates busy tone after remote onhook in basic call mode.

Command Default

Automatic busytone generation after remote disconnect is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The automatic busytone generation after remote disconnect in basic call mode feature is enabled and disabled per dial peer with the **tone busytone remote-onhook** command. The **tone busytone** command is available to all dial peer services. Each service determines whether to utilize or enable it. For STCAPP, only the Foreign eXchange Subscriber (FXS) loop-start port will enable this service.

Note The **tone busytone** command cannot coexist with the dialtone generation after remote-onhook feature. Because the **tone dialtone** is a default configuration, you must disable the feature using the **no tone dialtone** command before connfiguring the **tone busytone** command.

Use the **show dial-peer voice** command or the **show stcapp device voice** command to verify the feature is enabled.

Examples

The following example shows busytone generation after remote disconnect being configured:

```
Router(config-dial-peer)# tone busytone remote-onhook
```

Related Commands

Command	Description
show dial-peer voice	Displays information for voice dial peers.

Command	Description
tone dialtone	Enable automatic dial tone generation.
show stcapp device voice	Displays configuration information about STCAPP analog voice ports.

tone dialtone

To enable automatic dial-tone generation in basic call mode, use the **tone dialtone** command in dial peer configuration mode. To disable automatic dial-tone generation, use the **no** form of this command.

tone dialtone remote-onhook

no tone dialtone remote-onhook

Syntax Description

remote-onhook	Generates dial tone after remote onhook in basic call mode.

Command Default

Automatic dial-tone generation after remote disconnect is enabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

Use this command to generate immediate dial tone once a remote party disconnects, similar to what the user experiences in a PBX environment. If you disable this feature using the **no** form of this command, the user is required to go on hook or perform a hookflash to generate dial tone after the remote party disconnects in a basic two-part call scenario. This feature is supported on Skinny Client Control Protocol (SCCP) gateway controlled loop-start FXS ports only.

Examples

The following examples show that the automatic Dial Tone Generation After Remote Onhook feature is enabled. Because the dial tone generation after remote onhook feature is enabled by default, it does not display in the show running-config output.

```
Router# show running-config
service stcapp
 dial-peer voice 3001 pots
 port 1/1/1

Router# show dial-peer voice 3001
VoiceEncapPeer3001
 peer type = voice, system default peer = FALSE, information type = voice,
!
!
!
 in bound application associated: 'stcapp'
 dial tone generation after remote-onhook = enabled
```

```
Router# show stcapp device voice-port 1/1/1
Port Identifier:  1/1/1
!
Dialtone after remote-onhook feature: activated
```

The following examples show the dial tone generation after remote onhook feature disabled.

```
Router# show running-config
no tone dialtone remote-onhook
dial-peer voice 3002 pots
 service stcapp
 port 1/1/0
```

Related Commands

Command	Description
sccp	Enables SCCP and related applications.
show dial-peer voice	Displays information for voice dial peers.
show stcapp device	Displays configuration information about SCCP Telephony Control Application (STCAPP) analog voice ports.

tone incoming

To activate 2100-Hz answer (ANS) tone detection on either the IP or the PSTN side of the network and to disable the echo suppressor, use the **tone incoming** command in voice-service VoIP configuration mode or dial peer configuration mode. To deactivate tone detection and disable the echo suppressor, use the **no** form of this command.

tone incoming [**ip** | **pstn**] {{**ans-all auto-control** | **ans disable echo suppressor** | **anspr disable echo suppressor**}}

no tone incoming

Syntax Description

ip	(Optional) Specifies tone detection on the IP side of the network.
pstn	(Optional) Specifies tone detection on the PSTN side of the network.
ans auto-control	Detects ANS tone and enables standard actions for modem tones.
ans-all disable echo suppressor	Detects modem answer tones and disables echo suppressor.
anspr disable echo suppressor	Detects /ANS tone and disables echo suppressor.

Command Default

Tone incoming detection is not enabled.

Command Modes

Voice-service VoIP configuration
Dial peer configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command in voice-service VoIP or VoIP dial peer configuration mode to activate detection of all ANS, ANSam, and ANSpr tones and enable or disable echo canceller control. When this command is issued in voice-service VoIP configuration mode, all dial peers are globally configured unless a specific dial peer is configured for no tone incoming.

To deactivate all 2100-Hz ANS, ANSam, and ANSpr tone detection on either the IP or the PSTN side of the network, and enable the echo canceller, use the **no tone incoming** command in voice-service VoIP configuration or dial peer configuration mode.

If neither IP nor PSTN is specified, all ANS, ANSam, and ANSpr tones are detected on both sides of the network, and the echo suppressor is disabled in all cases.

The **tone incoming ip ans-all auto-control** command is equivalent to these two commands together:

- **tone incoming ip ans disable echo suppressor**
- **tone incoming ip anspr disable echo suppressor**

The **tone incoming pstn ans-all auto-control** command is equivalent to these two commands together:

- **tone incoming pstn ans disable echo suppressor**
- **tone incoming pstn anspr disable echo suppressor**

The **tone incoming ans-all auto-control** command is equivalent to these four commands together:

- **tone incoming ip ans disable echo suppressor**
- **tone incoming ip anspr disable echo suppressor**
- **tone incoming pstn ans disable echo suppressor**
- **tone incoming pstn anspr disable echo suppressor**

When modem tones from either the IP or PSTN direction are received, the echo canceller can be dynamically disabled to allow modem calls to pass through.

The IP tone detector feature applies only on the following NextPort platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850—and only with SIP and H.323 voice signaling. It does not apply to MGCP in dial peer configuration mode.

The gateway must be configured for G.711 codecs for the IP tone detector feature to work (see the "Examples" section).

To display the status of the echo canceller, use the **show port operational status** command.

Examples

The following example configures tone detection of ANS tones in voice-service VoIP configuration mode:

```
Router(conf-voi-serv)# tone incoming ip ans disable echo supressor
```

The following example configures tone detection of all incoming ANS, ANSam, and ANSpr tones on a dial peer:

```
Router(config-dial-peer)# tone incoming ip ans-all auto-control
```

Related Commands

Command	Description
tone incoming system	Sets a dial peer for tone incoming or no tone incoming detection.
show port operational status	Displays the status of the echo canceller.

tone incoming system

To set a dial peer for tone incoming or no tone incoming, use the **tone incoming system** command in VoIP dial peer configuration mode. To block the voice service VoIP settings for a dial peer, use the **no** form of this command.

tone incoming system

no tone incoming system

Syntax Description

This command has no arguments or keywords.

Command Default

The dial peer is set for tone incoming.

Command Modes

dial peer configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command in dial peer configuration mode to activate or deactivate tone detection and to enable echo canceller control. When modem tones from either the IP or PSTN directions are received. The echo canceller can be dynamically disabled to allow modem calls through. This command is used primarily to allow or to block global voice service VoIP configuration settings.

To block the voice service VoIP settings for a dial peer, use the **no tone incoming system** command.

Examples

The following example shows activating tone detection for a dial peer.

```
Router(config-dial-peer)# tone incoming system
```

The following example shows deactivating tone detection for a dial peer.

```
Router(config-dial-peer)# no tone incoming system
```

Related Commands

Command	Description
tone incoming ans disable echo suppressor	Activates ANS tone detection.
tone incoming anspr disable echo canceller	Activates ANSpr tone detection.

Command	Description
tone incoming ans-all auto-control	Activates ANS, ANSam, and ANSpr tone detection.
show port operational status	Displays the status of the echo canceller.

tone ringback alert-no-PI

To generate automatic ringback for the caller when no Progress Indicator (PI) alert has been received over the H.323 network, use the **tone ringback alert-no-PI** command in dial peer configuration mode. To disable automatic ringback, use the **no** form of this command.

tone ringback alert-no-PI

no tone ringback alert-no-PI

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, and Cisco 7200 series routers and on the Cisco AS5300 and Cisco AS5800 universal access servers.

Usage Guidelines

The **tone ringback alert-no-PI** command is used to generate ringback in an H.323 network when the attached device (for example, an ISDN device) cannot.

Examples

The following example activates ringback for a VoIP dial peer numbered 322:

```
router(config)# dial-peer voice 322 voip
router(config-dial-peer)# tone ringback alert-no-PI
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

transfer

To define a Feature Access Code (FAC) to access the Call Transfer feature in feature mode on analog phones connected to FXS ports, use the **transfer** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

transfer *keypad-character*

no transfer

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0—9, *, #). Default is #2.

Command Default

The default value is #2.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for Call Transfer from the default (#2) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Examples

The following example shows how to change the value of the feature code for the Call Transfer feature from the default (#2). With this configuration, a phone user presses hook flash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, the user presses hook flash to get a feature tone and then dials 22 to transfer the call; the user hears silence after the call is transferred.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# transfer 22
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.

translate

To apply a translation rule to manipulate dialed digits on an inbound POTS call leg, use the **translate** command in voice-port configuration mode. To remove the translation rule, use the **no** form of this command.

translate {**calling-number** | **called-number**} *name-tag*

no translate {**calling-number** | **called-number**} *name-tag*

Syntax Description

calling-number	Translation rule applies to the inbound calling party number.
called-number	Translation rule applies to the inbound called party number.
name-tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.

Command Default

No default behavior or values

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for VoIP Cisco AS5300, Cisco 7200, and Cisco 7500.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

A translation rule is a general-purpose digit-manipulation mechanism that performs operations such as automatically adding telephone area and prefix codes to dialed numbers.

Examples

The following example applies translation rule 21 to the POTS inbound calling-party number:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
voice-port 0:1
 translate calling-number 21
```

The following example applies translation rule 20 to the POTS inbound called-party number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
voice-port 0:1
 translate called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

translate (translation profiles)

To associate a translation rule with a voice translation profile, use the **translate** command in voice translation-profile configuration mode. To delete the translation rule from the profile, use the **no** form of this command.

translate {**called** | **calling** | **redirect-called** | **redirect-target**} *translation-rule-number*

no translate {**called** | **calling** | **redirect-called** | **redirect-target**} *translation-rule-number*

Syntax Description

called	Associates the translation rule with called numbers.
calling	Associates the translation rule with calling numbers.
redirect-called	Associates the translation rule with redirected called numbers.
redirect-target	Associates the translation rule with transfer-to numbers and call-forwarding final destination numbers.
translation-rule-number	Number of the translation rule to use for the call translation. Valid range is from 1 to 2147483647. There is no default value.

Command Default

No translation rule is associated with the translation profile.

Command Modes

Voice translation-profile configuration (cfg-translation-profile)

Command History

Release	Modification
12.0(7)XR1	This command was introduced on the Cisco AS5300.
12.0(7)XK	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented on the following platforms: Cisco 1750, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series.
12.1(2)T	This command was implemented on the Cisco MC3810.
12.2(11)T	This command was reconfigured for voice translation-profile configuration mode. The **redirect-called** keyword and *translation-rule-number* argument were added.
12.4(11)XJ	The **redirect-target** keyword was added.
12.4(15)T	The **redirect-target** keyword was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use this command as part of a voice translation-profile definition. Enter this command for each translation rule that is part of the profile definition.

Examples

The following example defines voice translation profile “sjmorning” with two translation rules: translation rule 15 for called numbers and translation rule 36 for calling numbers.

```
Router(config)# voice translation-profile sjmorning
Router(cfg-translation-profile)# translate called 15
Router(cfg-translation-profile)# translate calling 36
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation-rule.
show voice translation-profile	Displays the configuration of the translation-profile.
translation-profile (dial-peer)	Assigns a translation profile to a dial peer.
translation-profile (source group)	Assigns a translation profile to a source IP group.
translation-profile (trunk group)	Assigns a translation profile to a trunk group.
translation-profile (voice port)	Assigns a translation profile to a voice port.
translation-profile (voice service POTS)	Assigns a translation profile to an NFAS interface.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translate-outgoing

To apply a translation rule to manipulate dialed digits on an outbound POTS or VoIP call leg, use the **translate-outgoing command in** dial peer configuration mode. To disable the translation rule, use the **no** form of this command.

translate-outgoing {**calling-number** | **called-number**} *name-tag*

no translate-outgoing {**calling-number** | **called-number**} *name-tag*

Syntax Description

calling-number	Apply to the outbound calling party number.
called-number	Apply to the outbound called party number.
name-tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is 1 to 2147483647. There is no default value.

Command Default

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.2(1)T and implemented for VoIP on the Cisco 1750, Cisco AS5300, Cisco 7200, and Cisco 7500. support for the Cisco MC3810 is not included in this release.
12.1(2)T	This command is supported on the Cisco MC3810 in this release.

Examples

The following example applies translation rule 21 to the VoIP outbound calling number:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
 dial-peer voice 100 voip
 translate-outgoing calling-number 21
```

The following example applies translation rule 20 to the VoIP called number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
dial-peer voice 100 voip
 translate-outgoing called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

translation-profile (dial peer)

To assign a translation profile to a dial peer, use the **translation-profile** command in dial peer configuration mode. To delete the translation profile from the dial peer, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*

no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Defaults

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a dial peer.

Examples

The following example assigns the translation profile named "profile1" to handle translation of outgoing calls for a dial peer:

```
Router(config)# dial-peer voice 111 pots
Router(config-dial-peer)# translation-profile outgoing profile1
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (source group)

To assign a translation profile to a source IP group, use the **translation-profile** command in source group configuration mode. To delete the translation profile from the source IP group, use the **no** form of this command.

translation-profile incoming *name*

no translation-profile incoming *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
name	Name of the translation profile.

Command Default No default behavior or values

Command Modes Source group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **translation-profile** command to assign a predefined translation profile to a source IP group.

Examples The following example assigns the translation profile named "chicago" to handle translation of incoming calls for a voice source group:

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# translation-profile incoming chicago
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (trunk group)

To assign a translation profile to a trunk group, use the **translation-profile** command in trunk group configuration mode. To delete the translation profile from the trunk group, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*

no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default No default behavior or values

Command Modes Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **translation-profile** command to assign a predefined translation profile to a trunk group.

Examples The following example assigns the translation profile named “newyork” to handle translation of incoming calls for a trunk group:

```
Router(config)# trunk group 10
Router(config-trunk-group)# translation-profile incoming newyork
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (voice port)

To assign a translation profile to a voice port, use the **translation-profile** command in voice port configuration mode. To delete the translation profile from the voice port, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*

no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Voice port configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a voice port.

Examples

The following example assigns the translation profile named “chicago” to handle translation of incoming calls and a translation profile named “sanjose” to handle outgoing calls for a voice port:

```
Router(config)# voice-port 1/0/0
Router(config-voiceport)# translation-profile incoming chicago
Router(config-voiceport)# translation-profile outgoing sanjose
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (voice service POTS)

To assign a translation profile to a non-facility associated signaling (NFAS) interface, use the **translation-profile** command in voice service POTS configuration mode. To delete the translation profile from the interface, use the **no** form of this command.

translation-profile [**incoming | outgoing**] **controller** [**T1 | E1**] *unit-number name*

no translation-profile [**incoming | outgoing**] **controller** [**T1 | E1**] *unit-number name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
T1	T1 controller.
E1	E1 controller.
unit-number	Number of the controller unit.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Voice service POTS configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to an NFAS interface.

Examples

The following example assigns to an NFAS interface the translation profile named “delta1” to outgoing T1 calls on controller slot 3 and translation profile “alpha” to incoming T1 calls on controller slot 2:

```
Router(config)# voice service pots
Router(conf-voi-serv)# translation-profile outgoing controller T1 3 delta1
Router(conf-voi-serv)# translation-profile incoming controller T1 2 alpha
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-rule

To create a translation name and enter translation-rule configuration mode to apply rules to the translation name, use the **translation-rule** command in global configuration mode. To disable the translation rule, use the **no** form of this command.

translation-rule *name-tag*

no translation-rule *name-tag*

Syntax Description

name-tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for the following voice technologies on the following platforms: • VoIP Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoFR Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoATM Cisco 3600 series and Cisco MC3810
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for the following voice technology on the following platforms: VoIP (Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series)
12.1(2)T	This command was integrated ino Cisco IOS Release 12.1(2)T for the following voice technologies on the following platforms: • VoIP Cisco MC3810 • VoFR Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoATM Cisco 3600 series and Cisco MC3810
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command applies to all translation rules.

Examples

The following example creates translation rule 21 and applies a rule to it:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

transport

To configure the Session Initiation Protocol (SIP) user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP, Transport Layer Security (TLS) over TCP, or User Datagram Protocol (UDP) socket, use the **transport** command in SIP user agent configuration mode. To block reception of SIP signaling messages on a particular socket, use the **no** form of this command.

transport {**tcp tls** | **udp**}

no transport {**tcp tls** | **udp**}

Syntax Description

tcp tls	SIP user agent receives SIP messages on TLS over TCP port 5060.
udp	SIP user agent receives SIP messages on UDP port 5060.

Command Default

TCP, TLS over TCP, and UDP transport protocols are enabled.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XA	This command was implemented on Cisco AS5400 and Cisco AS5350 platforms.
12.2(2)XB1	This command was implemented on Cisco AS5850 platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms were not included in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release.
12.4(6)T	The **tls** keyword was added to the command.

Usage Guidelines

This command controls whether messages reach the SIP service provider interface (SPI). Setting **tls over tcp or udp** as the protocol causes this to be the protocol for which SIP user agents listen on port 5060.

To block reception of SIP signaling messages on a specific socket, use the **no** form of this command.

To reset this command to the default value, use the **no** form of this command.

Examples

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the UDP socket:

```
sip-ua
 transport udp
```

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the TLS over TCP socket:

```
sip-ua
 transport tcp tls
```

Related Commands

Command	Description
sip-ua	Enables the SIP user agent configuration commands.

transport switch

To enable switching between UDP and TCP transport mechanisms globally for large Session Initiation Protocol (SIP) messages, use the **transport switch** command in SIP configuration mode. To disable switching between UDP and TCP transport mechanisms globally for large SIP messages, use the **no** form of this command.

transport switch udp tcp

no transport switch udp tcp

Syntax Description

udp	Enables switching the transport mechanism from UDP on the basis of the size of the SIP request being greater than the MTU size.
tcp	Enables switching transport to TCP.

Command Default

Disabled.

Command Modes

SIP configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Switching between transports is provided globally on the router and also on an individual VoIP dial peer.

- Dial-peer mode. You can configure transport for a specific dial peer by using the **voice-class sip transport switch** command. The **voice-class sip transport switch command in** dial peer configuration mode takes precedence over the **transport switch** command in global configuration mode.
- SIP mode. You can configure transport globally by using the **transport switch** command. The **transport switch** command is considered only when there is no matching VoIP dial peer.

In a call forking scenario, if this command is configured, the configuration applies to all forks.

Examples

The following example enables switching of the transport from UDP to TCP:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# transport switch udp tcp
```

Related Commands

Command	Description
debug ccsip transport	Enables tracing of the SIP transport handler and the TCP or UDP process.
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip transport switch	Enables switching between transport mechanisms if the SIP message is larger than 1300 bytes for a specific dial peer.

trunk group

To define or modify the definition of a trunk group and to enter trunk group configuration mode, use the **trunk group** command in global configuration mode. To delete the trunk group, use the **no** form of this command.

trunk group *name*

no trunk group *name*

Syntax Description

name	Name of the trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **trunk group** command to assign a number or a name to a set of trunk characteristics. The set of characteristics, or profile, is assigned to specific trunks as part of the usual trunk configuration steps.

The **trunk group** command initiates the profile definition and switches from global configuration to trunk group configuration mode. Additional commands are available to construct the characteristics of the profile.

Up to 1000 trunk groups can be configured on the gateway provided that the gateway has sufficient memory to store the profiles. If you see the message "Trunk group name could not be added as the threshold has been reached", enter the **debug tgrm** command and check the number of trunk groups or check for insufficient memory.

Examples The following example assigns the number 5 to a trunk group profile:

```
Router(config)# trunk group 5
Router(config-trunk-group)# carrier-id allcalls
Router(config-trunk-group)# maxcalls voice 500 in
Router(config-trunk-group)# hunt-scheme round-robin even up
Router(config-trunk-group)# translation-profile incoming 3
Router(config-trunk-group)# translation-profile outgoing 2
Router(config-trunk-group)# exit
```

The following example assigns the name “newyork” to a trunk group profile:

```
Router(config)# trunk group newyork
Router(config-trunk-group)# carrier-id local
Router(config-trunk-group)# maxcalls voice 500
Router(config-trunk-group)# hunt-scheme least-idle
Router(config-trunk-group)# translation-profile incoming 1
Router(config-trunk-group)# translation-profile outgoing 12
Router(config-trunk-group)# exit
```

Related Commands

Command	Description
carrier-id (trunk group)	Identifies the carrier that owns the trunk group.
description (trunk group)	Permits a description to be associated with a trunk group.
hunt-scheme least-idle	Specifies the least-idle channel search method for incoming and outgoing calls.
hunt-scheme least-used	Specifies the least-used channel search method for incoming and outgoing calls.
hunt-scheme longest-idle	Specifies the longest-idle channel search method for incoming and outgoing calls.
hunt-scheme random	Specifies the random channel search method for incoming and outgoing calls.
hunt-scheme round-robin	Specifies the round-robin channel search method for incoming and outgoing calls.
hunt-scheme sequential	Specifies the sequential channel search method for incoming and outgoing calls.
max-calls	Specifies the number of incoming and outgoing voice and data calls that a trunk group can handle.
show trunk group	Displays the configuration of trunk groups.
translation-profile (trunk group)	Defines call number translation profiles for incoming and outgoing calls.

trunk-group (CAS custom)

To assign a channel-associated signaling (CAS) trunk to a trunk group, use the **trunk-group** command in CAS custom configuration mode. To delete the CAS trunk from the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]

no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Maximum length of the trunk group name is 63 alphanumeric characters.
preference-num	(Optional) Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

CAS custom configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **trunk-group** command to assign a CAS trunk as a member of a trunk group. This assignment provides the CAS trunk with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one CAS trunk is assigned to the same trunk group, the *preference-num* value determines the order in which the trunk group uses the interfaces. A *preference-num* value of 1 is the highest preference so that the trunk is used first; a value of 64 is the lowest preference so that the trunk is used last. If no value is entered for *preference-num*, the software assigns the trunk a preference of 65, which causes that trunk to be used after all other trunks are used.

If two CAS trunks have the same *preference-num*, the trunk that was configured first is used before the other trunk.

A CAS trunk can belong to only one trunk group.

If an interface is removed from the CAS trunk, the interface is removed automatically from the trunk group. A new nonprimary CAS interface is automatically a member of the same trunk group as its primary CAS interface.

Examples

The following example assigns two CAS interfaces to trunk group "westcoast". The preference value for DS0 group 2 is lower than for DS0 group 1; hence DS0 group 2 has a higher priority. Trunk group "westcoast" uses DS0 group 2 first.

```
Router(config)# controller T1 1/0
Router(config-controller)# ds0-group 1 timeslots 1-10 type e&m-fgd
Router(config-controller)# cas-custom 1
Router(config-controller)# trunk-group westcoast 5
Router(config-controller)# exit

Router(config)# controller T1 1/0
Router(config-controller)# ds0-group 2 timeslots 15-20 type e&m-fgd
Router(config-controller)# cas-custom 2
Router(config-controller)# trunk-group westcoast 3
Router(config-controller)# exit
```

Related Commands

Command	Description
show trunk group	Displays the configuration of a trunk group.

trunkgroup (dial peer)

To assign a dial peer to a trunk group for trunk group label routing, use the **trunkgroup** command in dial peer configuration mode. To delete the dial peer from the trunk group, use the **no** form of this command.

trunkgroup *name preference-num*

no trunkgroup *name*

Syntax Description

name	Label of the trunk group to use for the call. Valid trunk group names contain a maximum of 63 alphanumeric characters.
preference-num	Preference or priority of the trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default Preference-num is set lower than 64 (internally set to 65)

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into the Cisco IOS Release 12.2.
12.2(11)T	The *preference-num* argument was added.

Usage Guidelines Use the **trunkgroup** command to assign an outgoing dial peer as a member of one or more trunk groups. This assignment provides the dial peer with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If the dial peer is a member of more than one trunk group, use the *preference-num* value to set the order in which the trunk groups will be used for the dial peer. A *preference-num* value of 1 is the highest preference so that the trunk group is used first; a value of 64 is the lowest preference so that the trunk group is used last. If no value is entered for *preference-num*, the software assigns the trunk group a preference of 65, which causes that trunk group to be selected after all other trunks are used.

If two trunk groups have the same *preference-num*, the trunk group that was configured first is used before the other trunk group.

Examples In the following example, dial peer 112 should use the trunk group “east17” and trunk group “north5” for outbound dial peer matching. When selecting a trunk group, “north5” is used first because it has a higher preference than “east17”:

```
Router(config)# dial-peer voice 112 pots
Router(config-dial-peer)# trunkgroup east17 3
Router(config-dial-peer)# trunkgroup north5 1
```

Related Commands

Command	Description
debug dialpeer	Initiates dial peer debugging.
show dial-peer voice	Displays the dial peer configuration.
translation-profile (dial peer)	Defines call number translation profiles for incoming and outgoing calls.

trunk-group (interface)

To assign an ISDN PRI or Non-Facility Associated Signaling (NFAS) interface to a trunk group, use the **trunk-group** command in interface configuration mode. To delete the interface from the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]

no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Valid trunk group names contain a maximum of 63 alphanumeric characters.
preference-num	Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(11)T	The trunk-group identification was expanded to include alphanumeric characters using the *name* argument, and the *preference-num* argument was added.

Usage Guidelines

Use the **trunk-group** command to configure an ISDN PRI or Non-Facility Associated Signaling (NFAS) interface as a member of a trunk group. This assignment provides the interface with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one interface is assigned to the same trunk group, the *preference_num* value determines the order in which the trunk group uses the interfaces. A *preference-num* value of 1 is the highest preference so that the interface is used first; a value of 64 is the lowest preference so that the interface is used last. If no value is entered for *preference-num*, the software assigns the interface a preference of 65, which causes that interface to be selected after all other interfaces are used.

If two interfaces have the same *preference-num*, the interface that was configured first is used before the other interface.

An interface can belong to only one trunk group. Multiple interfaces can belong to the same trunk group.

If an NFAS interface group is assigned as a member of a trunk group, all the subinterfaces belong to that trunk group.

If a subinterface is removed from the NFAS group, the subinterface is removed automatically from the trunk group.

If a new nonprimary NFAS interface is added to the NFAS group, that interface automatically becomes a member of the same trunk group as its primary NFAS interface.

Examples

The following example assigns an ISDN interface to trunk group "eastern" with a preference of 3.

```
Router(config)# interface Serial2:23
Router(config-if)# no ip address
Router(config-if)# isdn switch-type primary-ni
Router(config-if)# isdn T306 30000
Router(config-if)# isdn T310 10000
Router(config-if)# no cdp enable
Router(config-if)# trunk-group eastern 3
Router(config-if)# exit
```

If another interface were assigned to trunk group "eastern" with preference of 1 or 2, the trunk group would use that interface before the one shown above.

Related Commands

Command	Description
show trunk group	Displays the configuration of the trunk group.

trunk-group (voice port)

To assign an analog voice port to a trunk group, use the **trunk-group** command in voice port configuration mode. To delete the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]

no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Maximum length of the trunk group name is 63 alphanumeric characters.
preference-num	Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default Preference-num is set lower than 64 (internally set to 65)

Command Modes Voice port configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **trunk-group** command to configure an analog voice port as a member of a trunk group. This assignment provides the voice port with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one voice port is assigned to the same trunk group, the *preference-num* value determines the order by which the trunk group uses the voice ports. A *preference-num* value of 1 is the highest preference so that the voice port is used first; a value of 64 is the lowest preference so that the voice port is used last. If no value is entered for *preference-num*, the software assigns the voice port a preference of 65, which causes that voice port to be selected after all other voice ports are used.

If two voice ports have the same *preference-num*, the voice port that was configured first is used before the other voice port.

A voice port can belong to only one trunk group. Multiple voice ports can belong to the same trunk group.

Examples The following example assigns voice port 1/0/0 and voice port 1/0/1 to trunk group “north5”. Trunk group “north5” uses voice port 1/0/1 before using voice port 1/0/0 because voice port 1/0/1 has preference 1, which is a higher priority than voice port 1/0/0, with preference 2.

```
Router(config)# voice port 1/0/0
Router(config-voiceport)# translation-profile incoming 7
Router(config-voiceport)# translation-profile outgoing 4
Router(config-voiceport)# trunk-group north5 2
Router(config-voiceport)# exit
```

```
Router(config)# voice port 1/0/1
Router(config-voiceport)# translation-profile incoming 3
Router(config-voiceport)# translation-profile outgoing 8
Router(config-voiceport)# trunk-group north5 1
Router(config-voiceport)# exit
```

Related Commands

Command	Description
show trunk group	Displays the configuration of a trunk group.

trunk-group-label (dial peer)

To specify a trunk group as the source or target of a call, use the **trunk-group-label** command in dial peer configuration mode. To delete the trunk group label, use the **no** form of this command.

trunk-group-label {**source** | **target**} *name*

no trunk-group-label {**source** | **target**} *name*

Syntax Description

source	Indicates the trunk group as the source of the incoming call.
target	Indicates the trunk group as the target of the outbound call.
name	Trunk group label. Maximum length of the trunk group label is 127 alphanumeric characters.

Command Default No default behavior or values

Command Modes Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines An originating gateway uses the source trunk group label as a matching key to route the call over an inbound dial peer. The terminating gateway uses the target trunk group label to select a dial peer for routing the outbound call over a POTS line.

If a dial peer has a source (or target) carrier ID already defined, then assigning a source (or target) trunk group label to that same dial peer overrides the source (or target) carrier ID. The same is true for the reverse: if a dial peer has a source (or target) trunk group label defined, then assigning a source (or target) carrier ID for that same dial peer overrides the source (or target) trunk group label.

The name of a trunk group label and carrier ID cannot be the same in dial peers.

Examples The following example shows that dial peer 112 should use trunk group label “north3” for inbound dial peer matching and trunk group label “east17” for outbound dial peer matching:

```
Router(config)# dial-peer voice 112 pots
Router(config-dial-peer)# trunk-group-label source north3
Router(config-dial-peer)# trunk-group-label target east17
```

Related Commands

Command	Description
carrier-id (dial peer)	Specifies the carrier associated with a VoIP call.
show dial-peer voice	Displays configuration information for dial peers.

trunk-group-label (voice source group)

To define a trunk group label in a source IP group, use the **trunk-group-label** command in voice source group configuration mode. To delete the trunk group label, use the **no** form of this command.

trunk-group-label {**source** | **target**} *name*

no trunk-group-label {**source** | **target**} *name*

Syntax Description

source	Indicates the trunk group as the source of the incoming call.
target	Indicates the trunk group as the target of the outbound call.
name	Trunk group label. Maximum length of the trunk group label is 127 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Voice source group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

A terminating gateway uses the source trunk group label as a search key to find a source IP group for the incoming VoIP call. The gateway uses the target trunk group label to select an outbound dial peer to route the call over a POTS line.

If a source IP group has a source (or target) carrier ID already defined, then assigning a source (or target) trunk group label to that same source IP group overrides the source (or target) carrier ID. The same is true for the reverse: if a source IP group has a source (or target) trunk group label defined, then assigning a source (or target) carrier ID for that same source IP group overrides the source (or target) trunk group label.

The name of a trunk group label and carrier ID of the same type (source or target) cannot be the same in the source IP group.

Examples

The following example shows that source IP group “alpha” uses trunk group “north3” to search for a source IP group for incoming VoIP calls and trunk group “east17” for outbound dial peer matching:

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# trunk-group-label source north3
Router(cfg-source-grp)# trunk-group-label target east17
```

Related Commands

Command	Description
carrier-id (dial peer)	Specifies the carrier associated with a VoIP call.
show voice source-group	Displays the configuration for voice source IP groups.

trustpoint (DSP farm profile)

To associate a trustpoint with a DSP farm profile, use the **trustpoint** command in DSP farm profile configuration configuration mode. To remove the association, use the **no** form of this command.

trustpoint *trustpoint-label*

no trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Label of the trustpoint to be associated with the digital signal processor (DSP) farm profile.

Command Default No trustpoints are associated with the DSP farm profile

Command Modes DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use this command to associate trustpoints with secure DSP farm profiles only. Use the **security** keyword of the **dspfarm profile** command to configure a secure DSP farm profile. If the trustpoint is not already configured, you are prompted to configure the trustpoint.

Examples The following example associates the trustpoint dspfarm with the DSP farm profile 101:

```
Router(config)# dspfarm profile 101 conference security
Router(config-dspfarm-profile)# trustpoint dspfarm
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for digital signal processor (DSP) farm services.

ttl

To set the expiration timer for advertisements, enter the **ttl** command in Annex G configuration mode. To reset to the default, use the **no** form of this command.

ttl *ttl-value*

no ttl

Syntax Description

ttl-value	Amount of time (in seconds) for which a route from a neighbor is considered valid. Range is from 1 to 2147483647. The default is 1800 (or 30 minutes).

Command Default 1800 seconds (30 minutes)

Command Modes Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The address templates or routes that are static to this Annex G border element (BE) can be advertised to its neighbors. A time-to-live (TTL) value is associated with each of the advertised routes. The TTL value indicates how long the neighbor should consider the routes valid. On expiration of the ttl, the neighbor must query the addressing information again.

Examples The following example shows a BE with a time-to-live value of 20 seconds.

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# ttl 20
```

Related Commands

Command	Description
call-router	Enables the Annex G BE configuration commands.
show call-router status	Displays the Annex G BE status.

type (settlement)

To point to the provider type and the specific settlement server, use the **type** command in settlement configuration mode. To disable this command, use the **no** form of this command.

type {**osp** | **uni-osp**}

no type

Syntax Description

osp	Enables the Open Settlement Protocol (OSP) server type.
uni-osp	Enables authentication of VoIP calls to the Public Switched Telephone Network (PSTN) using a single settlement server.

Command Default **osp**

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on Cisco 2600 series and Cisco 3600 series, and Cisco AS5300.
12.1(2)T	The **uni-osp** keyword was introduced.

Usage Guidelines This command defines the settlement server that is doing the accounting and enables the server to do the accounting.

Examples The following example enables authentication of VoIP calls to the PSTN using a single settlement server:

```
settlement 0
 type uni-osp
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Brings up the settlement provider and then shuts it down.
url	Specifies the Internet service provider (ISP) address.

type (voice)

To specify the E&M interface type, use the **type** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

type {**1** | **2** | **3** | **5**}

no type {**1** | **2** | **3** | **5**}

Syntax Description

1	Indicates the following lead configuration: • E—Output, relay to ground. • M—Input, referenced to ground.
2	Indicates the following lead configuration: • E—Output, relay to SG. • M—Input, referenced to ground. • SB—Feed for M, connected to –48V. • SG—Return for E, galvanically isolated from ground.
3	Indicates the following lead configuration: • E—Output, relay to ground. • M—Input, referenced to ground. • SB—Connected to –48V. • SG—Connected to ground.
5	Indicates the following lead configuration: • E—Output, relay to ground. • M—Input, referenced to –48V.

Command Default Type 1

Command Modes Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.
11.3(1)MA	This command was implemented on Cisco MC3810.

Usage Guidelines Use the **type** command to specify the E&M interface for a particular voice port. With **1**, the tie-line equipment generates the E-signal to the PBX type grounding the E-lead. The tie-line equipment detects the M-signal by detecting current flow to ground. If you select **1**, a common ground must exist between the line equipment and the PBX.

With **2**, the interface requires no common ground between the equipment, thereby avoiding ground loop noise problems. The E-signal is generated toward the PBX by connecting it to SG. The M-signal is indicated by the PBX connecting it to SB. While Type 2 interfaces do not require a common ground, they do have the tendency to inject noise into the audio paths because they are asymmetrical with respect to the current flow between devices.

Note E&M Type 4 is not a supported option. However, Type 4 operates similarly to Type 2 except for the M-lead operation. On Type 4, the M-lead states are open/ground, compared to Type 2, which is open/battery. Type 4 can interface with Type 2. To use Type 4 you can set the E&M voice port to Type 2 and perform the necessary M-lead rewiring.

With **3**, the interface operates the same as Type 1 interfaces with respect to the E-signal. The M-signal, however, is indicated by the PBX connecting it to SB on assertion and alternately connecting it to SG during inactivity. If you select **3**, a common ground must be shared between equipment.

With **5**, the Type 5 line equipment indicates E-signal to the PBX by grounding the E-lead. The PBX indicates M-signal by grounding the M-lead. A Type 5 interface is quasi-symmetrical in that while the line is up, current flow is more or less equal between the PBX and the line equipment, but noise injection is a problem.

Examples

The following example selects Type 3 as the interface type for the voice port:

```
voice-port 1/0/0
 type 3
```

Cisco IOS Voice Commands: U

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

unbundle vfc

To unbundle DSPWare from the VCWare and configure the default file and capability lists with default values, use the **unbundle vfc** command in privileged EXEC mode.

unbundle [**high-complexity** | **medium-complexity**] **vfc** *slot-number*

Syntax Description

high-complexity	(Optional) Unbundles the high-complexity firmware set.
medium-complexity	(Optional) Unbundles the medium-complexity firmware set.
slot-number	Voice feature card (VFC) slot number.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco AS5300.
12.0(2)XH	The **high-complexity** and **medium-complexity** keywords were added.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

VFCs come with a single bundled image, VCWare, stored in VFC Flash memory. Use the **unbundle vfc** command to unbundle this bundled image into separate files, which are then written to Flash memory. When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for that version of VCWare. The default file list includes the files to be used to boot up the system. The capability list defines the available voice codecs for H.323 capability negotiation. These files are used during initial card configuration and for subsequent firmware upgrades.

Before unbundling a VFC software image that you have just copied over to VFC Flash, use the **clear vfc** command. Unbundling a DSP firmware set rewrites the default-file and capabilities lists. After unbundling, you must reload the router for any changes to take effect.

Examples

The following example unbundles the high-complexity firmware set into slot 2:

```
Router# unbundle high-complexity vfc 2
```

Related Commands

Command	Description
copy flash vfc	Copies a new version of VCWare from the Cisco AS5300 motherboard to VFC Flash memory.
copy tftp vfc	Copies a new version of VCWare from a TFTP server to VFC Flash memory.

url

To configure the Internet service provider (ISP) address, use the **url** command in settlement configuration mode. You can configure the address type multiple times. To disable the address, use the **no** form of this command.

url *url-address*

no url *url-address*

Syntax Description

url-address	URL address. A valid URL address is as follows: http://*fully qualified domain name*[:*port*]/[*URL*]

Command Default No default behavior or values

Command Modes Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on Cisco 2600 series and Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	The settlement configuration for this command was modified. The settlement provider must be shutdown before the **url** command is entered.

Usage Guidelines You can configure the address type multiple times. If you configure multiple URLs for the settlement server, the gateway attempts to send the request to each URL in the order in which you configured these addresses.

If the first URL is unsuccessful, the gateway tries the next URL. If the first URL becomes available, the gateway does not switch back until it loops through the list of URLs, for example:

```
url http://servicepoint1.com
url http://servicepoint2.com
url http://servicepoint3.com
```

If http://servicepoint1.com fails, the gateway sends the request to http://servicepoint2.com. If http://servicepoint1.com comes back online, the gateway continues to send requests to http://servicepoint2.com. Later on, if http://servicepoint2 is down, the gateway sends requests to http://servicepoint3.com.

When http://servicepoint3.com is down the gateway routes its requests back to http://servicepoint1.com.

Examples

The following example shows four URLs configured for the settlement server:

```
settlement 0
 url http://1.2.3.4/
 url http://1.2.3.4:80/
 url https://1.2.3.4:4444/
 url https://yourcompany.com:443/
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Brings up the settlement provider and then shuts it down.
type	Specifies the provider type.

url (SIP)

To configure URLs to either the Session Initiation Protocol (SIP), SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls, use the **url** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

url {**sip** | **sips** | **tel** [**phone-contex**t]}

no url

Syntax Description

sip	Generates URLs in SIP format for VoIP calls.
sips	Generates URLs in SIPS format for VoIP calls.
tel	Generates URLs in TEL format for VoIP calls.
phone-context	(Optional) Appends the phone-context parameter to the TEL URL.

Command Default

SIP URLs

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.4(6)T	The **sips** keyword was added.
12.4(22)YB	The **phone-context** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice call connections.

The **voice-class sip url** command takes precedence over the **url** command configured in SIP global configuration mode. However, if the **voice-class sip url** command is configured with the **system** keyword, the gateway uses what was globally configured with the **url** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example generates URLs in SIP format:

```
voice service voip
sip
 url sip
```

The following example generates URLs in SIPS format:

```
voice service voip
sip
 url sips
```

The following example generates URLs in TEL format:

```
voice service voip
sip
 url tel
```

The following example generates URLs in TEL format and appends the phone-context parameter:

```
voice service voip
sip
 url tel phone-context
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip url	Generates URLs in the SIP, SIPS, or TEL format.

usage-indication

To enter the Annex G neighbor usage mode used to configure optional usage indicators, use the **usage-indication** command in Annex G neighbor configuration mode. To return to the default setting, use the **no** form of this command.

usage-indication

no usage-indication

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Annex G neighbor

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use **usage-indication** command to enter the mode to set usage indication characteristics. Repeat this command for each border element neighbor that you configure.

Note The **no shutdown** command must be used to enable each service relationship.

Examples The following example shows how to enter the Annex G neighbor usage mode:

```
doc-rtr3(config-nxg-neigh-usg)# usage-indication
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines for how long a border element will attempt delivery.
shutdown	Enables or disables the border element.

use-proxy

To enable proxy communications for calls between local and remote zones or the H.225 Annex G border element, use the **use-proxy** command in gatekeeper configuration mode. To remove either a proxy configuration entry for a remote zone or the H.225 Annex G border element, to disable proxy communications between local and remote zones or H.225 Annex G border element, use the **no** form of this command.

use-proxy *local-zone-name* {**default** | **h323-annexg** | **remote-zone** *remote-zone-name*} {**inbound-to** | **outbound-from**} {**gateway** | **terminal**}

no use-proxy *local-zone-name* {**default** | h323-annexg | **remote-zone** *remote-zone-name*} [{**inbound-to** | **outbound-from**} {**gateway** | **terminal**}]

Syntax Description

local-zone-name	Name or zone name of the gatekeeper, which is usually the fully domain-qualified host name of the gatekeeper.
default	Default proxy policy for all calls that are not defined by a **use-proxy** command with the **remote-zone** keyword or **h323-annexg** keyword.
h323-annexg	Proxy policy for calls to or from the H.225 Annex G border element co-located with the gatekeeper.
remote-zone *remote-zone-name*	Proxy policy for calls to or from a specific remote gatekeeper or zone.
inbound-to	Proxy policy as it applies to calls that are inbound to the local zone from a remote zone. Each **use-proxy** command defines the policy for only one direction.
outbound-from	Proxy policy as it applies to calls that are outbound from the local zone to a remote zone. Each **use-proxy** command defines the policy for only one direction.
gateway	Type of local device to which the policy applies. The **gateway** option applies the policy only to local gateways.
terminal	Type of local device to which the policy applies. The **terminal** option applies the policy only to local terminals.

Command Default

The local zone uses proxy for both inbound and outbound calls to and from the local H.323 terminals only. Proxy is not used for both inbound and outbound calls to and from local gateways. For releases prior to Cisco IOS Release 12.3(7)T, both inbound and outbound calls using the H.225 Annex G border element do not use the proxy.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.3(7)T	The **h323-annexg** keyword was added.

Usage Guidelines

This command replaces the **zone access** command used in previous versions of the gatekeeper. When a previous version of a gatekeeper is upgraded, any **zone access** commands are translated to **use**-**proxy** commands. You can use the **show gatekeeper zone status** command to see the gatekeeper proxy configuration.

If the domain name is cisco.com, the gatekeeper name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the name of the gatekeeper for each zone should be a unique string.

Examples

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls from remote zones tokyo.xyz.com and milan.xyz.com to gateways in its local zone. The sj.xyz.com zone is also configured to use a proxy for outbound calls from gateways in its local zone to remote zones tokyo.xyz.com and milan.xyz.com.

```
use-proxy sj.xyz.com remote-zone tokyo.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone tokyo.xyz.com outbound-from gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com outbound-from gateway
```

Because the default mode disables proxy communications for all gateway calls, only the gateway calls listed above can use the proxy.

In the following example, the local zone sj.xyz.com uses a proxy for only those calls that are outbound from H.323 terminals in its local zone to the specified remote zone germany.xyz.com:

```
no use-proxy sj.xyz.com default outbound-from terminal
use-proxy sj.xyz.com remote-zone germany.xyz.com outbound-from terminal
```

Note Any calls inbound to H.323 terminals in the local zone sj.xyz.com from the remote zone germany.xyz.com use the proxy because the default applies.

The following example removes one or more proxy statements for the remote zone germany.xyz.com from the proxy configuration list:

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com
```

This command removes all special proxy configurations for the remote zone germany.xyz.com. After you enter a command like this, all calls between the local zone (sj.xyz.com) and germany.xyz.com are processed according to the defaults defined by any **use**-**proxy** commands that use the **default** option.

To prohibit proxy use for inbound calls to H.323 terminals in a local zone from a specified remote zone, enter a command similar to the following:

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com inbound-to terminal
```

This command overrides the default and disables proxy use for inbound calls from remote zone germany.xyz.com to all H.323 terminals in the local zone sj.xyz.com.

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls and outbound calls that use the H.225 Annex G border element co-located with the gatekeeper:

```
use-proxy sj.xyz.com h323-annexg inbound-to gateway
use-proxy sj.xyz.com h323-annexg outbound-from gateway
```

In the following example, the local zone sj.xyz.com is configured not to use a proxy for inbound calls and outbound calls that use the H.225 Annex G border element co-located with the gatekeeper:

```
no use-proxy sj.xyz.com h323-annexg inbound-to terminal
no use-proxy sj.xyz.com h323-annexg outbound-from terminal
```

The following example removes one or more proxy statements for the H.225 Annex G border element from the proxy configuration list:

```
no use-proxy sj.xyz.com h323-annexg
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.

user-id

To match a call based on the user-id field in the Session Initiation Protocol (SIP) uniform resource identifier (URI), use the **user-id** command in voice URI class configuration mode. To remove the match pattern, use the **no** form of this command.

user-id *username-pattern*

no user-id

Syntax Description

username-pattern	Cisco IOS regular expression pattern to match against the user-id field in a SIP URI. Can be up to 32 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- You can use this command only in a voice class for SIP URIs.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples

The following example defines a voice class that matches on the user-id field in a SIP URI:

```
voice class uri r100 sip
 user-id abc123
```

Related Commands

Command	Description
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.

Command	Description
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

Cisco IOS Voice Commands: V

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

vad (dial peer)

To enable voice activity detection (VAD) for the calls using a particular dial peer, use the **vad** command in dial peer configuration mode. To disable VAD, use the **no** form of this command.

vad [**aggressive**]

no vad [**aggressive**]

Syntax Description

aggressive	Reduces noise threshold from –78 to –62 dBm. Available only when session protocol multicast is configured.

Command Default

VAD is enabled

Aggressive VAD is enabled in multicast dial peers

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
12.0(4)T	This command was implemented as a dial-peer command on Cisco MC3810 (in prior releases, the **vad** command was available only as a voice-port command).
12.2(11)T	The **aggressive** keyword was added.

Usage Guidelines

Use this command to enable voice activity detection. With VAD, voice data packets fall into three categories: speech, silence, and unknown. Speech and unknown packets are sent over the network; silence packets are discarded. The sound quality is slightly degraded with VAD, but the connection monopolizes much less bandwidth. If you use the **no** form of this command, VAD is disabled and voice data is continuously sent to the IP backbone. When configuring voice gateways to handle fax calls, VAD should be disabled at both ends of the IP network because it can interfere with the successful reception of fax traffic.

When the **aggressive** keyword is used, the VAD noise threshold is reduced from –78 to –62 dBm. Noise that falls below the –62 dBm threshold is considered to be silence and is not sent over the network. Additionally, unknown packets are considered to be silence and are discarded.

Examples

The following example enables VAD for a Voice over IP (VoIP) dial peer, starting from global configuration mode:

```
dial-peer voice 200 voip
 vad
```

Related Commands

Command	Description
comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
dial-peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
vad (voice-port)	Enables VAD for the calls using a particular voice port.

vad (SPA-DSP)

To enable or disable voice activity detection (vad) settings configured locally irrespective of the external vad settings, use the **vad** command in config dspfarm profile mode.

vad {**on** | **off**} **override**

Syntax Description

on	Enables the local vad settings irrespective of the external vad settings.
off	Disables the local vad settins irrespective of the external vad settings.
override	Overrides the external vad settings with local vad configuration details.

Command Default By default, VAD is enabled.

Command Modes DSP Farm Profile Configuration Mode (config-dspfarm-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines Use this command to enable voice activity detection locally irrespective of external VAD settings. With VAD, voice data packets fall into three categories: speech, silence, and unknown. Speech and unknown packets are sent over the network; silence packets are discarded. The sound quality is slightly degraded with VAD, but the connection monopolizes much less bandwidth. If you disable VAD, voice data is continuously sent to the IP backbone.

Examples The following example enables VAD and overrides external vad settings with local vad settings:

```
Router(config)# dspfarm profile 1
Router(config-dspfarm-profile)# vad on override
Router(config-dspfarm-profile)# do show running-config
!!!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 588
 associate application SBC
 vad on override
!
```

The following example disables local vad settings and overrides external vad setting configuration:

```
Router(config)# dspfarm profile 1
Router(config-dspfarm-profile)# vad off override
Router(config-dspfarm-profile)# do show running-config
!!!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 588
 associate application SBC
 vad off override
!
```

Related Commands

Command	Description
dsp services dspfarm	Enables the DSP-farm services.
dspfarm profile	Enters the DSP farm profile configuration mode, and defines a profile for the DSP farm services.
show dspfarm (SPA-DSP)	Displays DSP farm service information, such as operational status and DSP resource allocation for transcoding.

vbd-playout-delay

To configure the voice-band-detection playout-delay buffer on a Cisco router, use the **vbd-playout-delay** command in voice service session configuration mode. To disable the buffer, use the **no** form of this command.

vbd-playout-delay {**maximum** *milliseconds* | **minimum** *milliseconds* | **mode** {**fixed** [**no-timestamps**] | **passthrough**}| **nominal** *milliseconds*}

no vbd-playout-delay

Syntax Description

maximum	Sets the maximum playout buffer delay, in milliseconds (ms). Range: 40 to 1000. Default: 1000.
milliseconds	Delay time, in milliseconds (ms).
minimum	Sets the minimum playout buffer delay, in ms. Range: 10 to 40. Default: 40.
mode	Configures voice-band-detection playout buffer adaptation mode.
fixed	Sets the jitter buffer to a constant delay.
no-timestamps	(Optional) Fixes the jitter buffer at a constant delay without time stamps.
passthrough	Sets the jitter buffer passthrough mode for clock compensation.
nominal	Sets the nominal playout buffer delay, in ms. Range: 10 to 1000. Default: 60.

Defaults

The voice-band-detection playout-delay buffer is disabled.

Command Modes

Voice service session configuration (conf-voi-serv-sess)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	This command was modified. • The minimum time range value was changed from 4 to 1700 ms to a range of 10 to 40 ms. The default value 4 was increased to 40 ms. • The maximum time value was decreased from 1700 to 1000 ms and the default of 200 was increased to 1000 ms. • The nominal time range value was changed from 0 to 1500 ms to a range of 10 to 1000 ms. The default value of 100 was decreased to 60 ms.
12.4(24)T6	This command was modified. The **no-timestamps** keyword was added and **passthrough** keyword usage guidelines were clarified.

Usage Guidelines

Use this command to set the playout jitter buffer. When a voice band is detected, the call uses the G.711 codec, and the playout delay values that you set are picked up. The original voice-call parameters are restored after the fax or modem call is completed. The **no-timestamps** keyword sets the jitter buffer at a constant delay without reading time stamps.

Note The **passthough** keyword is a special mode used to handle clock drifting properly. We recommend this keyword only when instructed by your Cisco representative.

Examples

The following example configures ATM adaptation layer 2 (AAL2) voice-band-detection playout-delay adaptation mode and sets the mode to fixed:

```
voice service voatm
session protocol aal2
 vbd-playout-delay mode fixed
```

The following example configures AAL2 voice-band-detection playout-delay adaptation mode and sets the mode at a constant delay without timestamps:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay mode fixed no-timestamps
```

The following example sets the nominal AAL2 voice-band-detection playout-delay buffer to 12 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay nominal 12
```

The following example sets the AAL2 voice-band-detection playout-buffer delay to a maximum of 55 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay maximum 55
```

The following example sets the AAL2 voice-band-detection playout-buffer delay to a minimum of 22 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay minimum 22
```

Related Commands

Command	Description
voice-service	Specifies the voice encapsulation type and enters voice service configuration mode.

vbr-rt

To configure the real-time variable bit rate (VBR) for VoATM voice connections, use the **vbr-rt** command in the appropriate configuration mode. To disable VBR for voice connections, use the **no** form of this command.

vbr-rt *peak-rate average-rate burst*

no vbr-rt

Syntax Description

peak-rate	Peak information rate (PIR) for the voice connection, in kbps. If it does not exceed your carrier's line rate, set it to the line rate. Range is from 56 to 10000.
average-rate	Average information rate (AIR) for the voice connection in kbps.
burst	Burst size, in number of cells. Range is from 0 to 65536.

Command Default

No real-time VBR settings are configured

Command Modes

For an ATM permanent virtual connection (PVC) or switched virtual circuit (SVC): Interface-ATM-VC configuration

For a virtual circuit (VC) class: VC-class configuration

For ATM VC bundle members: Bundle-vc configuration

Command History

Release	Modification
12.0	This command was introduced on Cisco MC3810.
12.1(5)XM	This command was implemented on Cisco 3600 series routers and modified to support Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command configures traffic shaping between voice and data PVCs. Traffic shaping is required so that the carrier does not discard calls. To configure voice and data traffic shaping, you must configure the peak, average, and burst options for voice traffic. Configure the burst value if the PVC will carry bursty traffic. Peak, average, and burst values are needed so that the PVC can effectively handle the bandwidth for the number of voice calls.

Calculate the minimum peak, average, and burst values for the number of voice calls as follows:

Peak Value

Peak value = (2 x the maximum number of calls) x 16K = _____

Average Value

Calculate according to the maximum number of calls that the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps:

- For VoIP:
  - G.711 with 40- or 80-byte sample size:

    Average value = max calls x 128K = _____
  - G.726 with 40-byte sample size:

    Average value = max calls x 85K = _____
  - G.729a with 10-byte sample size:

    Average value = max calls x 85K = _____
- For VoATM adaptation layer 2 (VoAAL2):
  - G.711 with 40-byte sample size:

    Average value = max calls x 85K = _____
  - G.726 with 40-byte sample size:

    Average value = max calls x 43K = _____
  - G.729a with 10-byte sample size:

    Average value = max calls x 43K = _____

If voice activity detection (VAD) is enabled, bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less.

Burst Value

Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows:

- Minimum burst size = 4 x number of voice calls = _____
- Maximum burst size = maximum allowed by the carrier = _____

When you configure data PVCs that will be traffic shaped with voice PVCs, use aal5snap encapsulation and calculate the overhead as 1.13 times the voice rate.

Examples

The following example configures the traffic-shaping rate for ATM PVC 20. Peak, average, and burst rates are calculated based on a maximum of 20 calls on the PVC.

```
pvc 20
 encapsulation aal5mux voice
 vbr-rt 640 320 80
```

Related Commands

Command	Description
encapsulation aal5	Configures the AAL and encapsulation type for an ATM PVC, SVC, or VC class.

vcci

To identify a permanent virtual circuit (PVC) to the call agent, use the **vcci** command in ATM virtual circuit (VC) configuration mode. To restore the default value, use the **no** form of this command.

vcci *pvc-identifier*

no vcci

Syntax Description

pvc-identifier	Identifier for the PVC. Range is from 0 to 32767. There is no default value.

Command Default

No default behavior or values

Command Modes

ATM virtual circuit configuration mode

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

The *pvc-identifier argument* is a unique 15-bit value for each PVC. The call agent sets up a call with the gateway by specifying the PVC using the *pvc-identifier.*

Examples

The following example shows how to assign a PVC identifier:

```
Router(config-if-atm-vc)# vcci 5278
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
pvc	Creates an ATM PVC for voice traffic.

video codec (dial peer)

To assign a video codec to a VoIP dial peer, use the **video codec** command in dial peer configuration mode. To remove a video codec, use the **no** form of this command.

video codec {**h261** | **h263** | **h263+** | **h264**}

no video codec

Syntax Description

h261	Video codec H.261
h263	Video codec H.263
h263+	Video codec H.263+
h264	Video codec H.264

Command Default No video codec is configured.

Command Modes Dial peer configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to configure a video codec for a VoIP dial peer. If no video codec is configured, the default is transparent codec operation between the endpoints.

Examples The following example shows configuration for video codec H.263+ on VoIP dial peer 30:

```
dial-peer voice 30 voip
 video codec h263+
```

Related Commands

Command	Description
video codec (voice-class)	Specifies a video codec for a voice class.

video codec (voice class)

To specify a video codec for a voice class, use the **video codec** command in voice class configuration mode. To remove the video codec, use the **no** form of this command.

video codec {**h261 | h263 | h263+ | h264**}

no video codec {**h261 | h263 | h263+ | h264**}

Syntax Description

h261	Apply this preference to video codec H.261
h263	Apply this preference to video codec H.263
h263+	Apply this preference to video codec H.263+
h264	Apply this preference to video codec H.264

Command Default No video codec is configured.

Command Modes Voice class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to specify one or more video codecs for a voice class.

Examples The following example shows configuration for voice class codec 10 with two audio codec preferences and three video codec preferences:

```
voice class codec 10
 codec preference 1 g711alaw
 codec preference 2 g722
 video codec h261
 video codec h263
 video codec h264
```

Related Commands

Command	Description
video codec (dial peer)	Specifies a video codec for a VoIP dial peer.

video screening

To enable transcoding and transsizing between two call legs when configuring SIP, use the **video screening** command in foice service SIP configuration mode. To disable transcoding and transsizing, use **no** form of this command.

video screening

no video screening

Syntax Description

This command has no arguments or keywords.

Command Default

Video screening is disabled.

Command Modes

Voice service SIP configuration.

Command History

Release	Modification
15.1(4)M	The command was introduced.

Usage Guidelines

Use this command to enable conversion of video streams if there is a mismatch between two call legs.

Examples

The following example enters the voice-card configuration mode and enables video screening:

```
Router(config)# voice service voip
Router(config-voicecard)# sip
Router((conf-serv-sip)# video screening
```

Related Commands

Command	Description
codec profile	Defines the video capabilities needed for video endpoints.
video codec	Assigns a video codec to a VoIP dial peer.

vmwi

To enable DC voltage or FSK visual message-waiting indictator (VMWI) on a Cisco VG224 onboard analog FXS voice port, use the **vmwi** command in voice-port configuration mode. To reset VMWI to default, use the **no** form of this command.

vmwi {**dc-voltage** | **fsk**}

no vmwi

Syntax Description

dc-voltage	DC voltage VMWI is enabled on this FXS port.
fsk	FSK VMWI is enabled on this FXS port. Default.

Command Default

FSK VMWI is enabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command with the **dc-voltage** keyword enables the message-waiting lamp to flash on an analog phone that requires DC voltage to activate a visual indicator.

This command with the **fsk** keyword enables the message-waiting lamp to flash on an analog phone that requires an FSK message to activate a visual indicator.

DC Voltage VMWI is supported for the SCCP telephony control (STC) application only. For all other applications, such as MGCP, FSK will be used even if you configure the **vmwi dc-voltage** command on the voice gateway.

Examples

The example shows how to enable DC Voltage VMWI on port 2/0 on a Cisco VG224.

```
Router(config)#voice-port 2/0
Router(config-voiceport)#vmwi dc-voltage
Router(config-voiceport)#end
```

Related Commands

Command	Description
stcapp	Enables basic SCCP call-control features for FXS analog ports on Cisco IOS voice gateways

vofr

To enable Voice over Frame Relay (VoFR) on a specific data-link connection identifier (DLCI) and to configure specific subchannels on that DLCI, use the **vofr** command in frame relay DLCI configuration mode. To disable VoFR on a specific DLCI, use the **no** form of this command.

Switched Calls

vofr [**data** *cid*] [**call-control** [*cid*]]

no vofr [**data** *cid*] [**call-control** [*cid*]]

Switched Calls to Cisco MC3810 Multiservice Concentrators Running Cisco IOS Releases Release Before 12.0(7)XK and Release 12.1(2)T

vofr [**cisco**]

no vofr [**cisco**]

Cisco-Trunk Permanent Calls

vofr data *cid* **call-control** *cid*

no vofr data *cid* **call-control** *cid*

FRF.11 Trunk Calls

vofr [**data** *cid*] [**call-control** *cid*]

no vofr [**data** *cid*] [**call-control** *cid*]

Syntax Description

data	(Required for Cisco-trunk permanent calls. Optional for switched calls.) Selects a subchannel (CID) for data other than the default subchannel, which is 4.
cid	(Optional) Specifies the subchannel to be used for data. Range is from 4 to 255. The default is 4. If **data** is specified, enter a valid CID.
call-control	(Optional) Reserves a subchannel for call-control signaling.
cisco	(Optional) Cisco proprietary voice encapsulation for VoFR with data is carried on CID 4 and call-control on CID 5.
cid	(Optional) Specifies the subchannel to be used for call-control signaling. Valid range is from 4 to 255. The default is 5. If **call-control** is specified and a CID is not entered, the default CID is used.

Command Default

Disabled

Command Modes

Frame relay DLCI configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	The use of the **cisco** option was modified. Beginning in this release, use the **cisco** option only when configuring connections to Cisco MC3810 running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Table 244 lists the different options of the **vofr** command and which combination of options is used beginning in Cisco IOS Release 12.0(7)XK and Release 12.1(2)T.

Table 244 Combinations of the vofr Command

Type of Call	Command Combination to Use
Switched call (user dialed or auto-ringdown) to other routers supporting VoFR	**vofr** [**data** *cid*] [**call-control** [*cid*]][1]
Cisco-trunk permanent call (private-line) to other routers supporting VoFR	**vofr data** *cid* **call-control** *cid*
FRF.11 trunk call (private-line) to other routers supporting VoFR	**vofr** [**data** *cid*] [**call-control** *cid*][2]

1. The recommended form of this command to use is **vofr data 4 call-control 5**.
2. For FRF.11 trunk calls, the call-control option is not required. It is required only if you mix FRF.11 trunk calls with other types of voice calls on the same PVC.

Examples

The following example, beginning in global configuration mode, shows how to enable VoFR on serial interface 1/1, DLCI 100. The example configures CID 4 for data; no call-control CID is defined.

```
interface serial 1/1
 frame-relay interface-dlci 100
 vofr
```

To configure CID 4 for data and CID 5 for call-control (both defaults), enter the following command:

```
vofr call-control
```

To configure CID 10 for data and CID 15 for call-control, enter the following command:

```
vofr data 10 call-control 15
```

To configure CID 4 for data and CID 15 for call-control, enter the following command:

```
vofr call-control 15
```

To configure CID 10 for data and CID 5 for call-control, enter the following command:

```
vofr data 10 call-control
```

To configure CID 10 for data with no call-control, enter the following command:

```
vofr data 10
```

Related Commands

Command	Description
class	Assigns a VC class to a PVC.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface.

voice

To enable voice resource pool services for resource pool management, use the **voice** command in service profile configuration mode. To disable voice services, use the **no** form of this command.

voice

no voice

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Service profile configuration mode

Command History

Release	Modification
12.2(2)XA	This command was introduced on the Cisco AS5350 and AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows that voice service is available and enables voice resource pool service using the **voice** command in service profile configuration mode:

```
Router(config)# resource-pool profile service voip

Router(config-service-profile)# ?
  Service Profile Configuration Commands:
  default   Set a command to its defaults
  exit      Exit from resource-manager configuration mode
  help      Description of the interactive help system
  modem     Configure modem service parameters
  no        Negate a command or set in its defaults
  voice     Configure voice service parameters

Router(config-service-profile)# voice
```

Related Commands

Command	Description
resource-pool enable	Enables resource pool management.
resource-pool profile service voip	Defines the VoIP service profile for resource pool management.

voicecap configure

To apply a voicecap on NextPort platforms, use the **voicecap configure** command in voice-port configuration mode. To remove a voicecap, use the **no** form of this command.

voicecap configure {*name*}

no voicecap configure {*name*}

Syntax Description

name	Designates which voicecaps to use on this voice port.

Command Default No default values or behavior

Command Modes Voice-port configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines The character value for the *name* argument must be identical to the value entered when you created the voicecap using the **voicecap entry** command.

Examples The following example configures a voicecap with the name qualityERL:

```
Router> enable
Router# configure terminal
Router(config)# voicecap entry qualityERL v270=120
Router(config)# voice-port 3/0:D
Router(config-voiceport)# voicecap configure qualityERL
```

Related Commands

Command	Description
voicecap entry	Creates a voicecap on NextPort platforms.

voicecap entry

To create a voicecap, use the **voicecap entry** command in global configuration mode. To disable a voicecap, use the **no** form of this command.

voicecap entry [*name string*]

no voicecap entry [*name string*]

Syntax Description

name string	(Optional) A word and a string of characters that uniquely identify a voicecap. • The *name* argument specifies a unique identifier for a voicecap. • The *string* argument specifies one or more voicecap register entries, similar to a modemcap. Each entry is of the form **v***index*=*value*, where *index* refers to a specific V register, and *value* designates the value for that V register.

Command Default

No voice caps can be applied to configure firmware.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.4(4)XC	This command was modified to include GSMAMR-NB codec capability.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command configures firmware through voicecap strings. This command allows you to assign values to specific registers. Voicecaps are applied to specific voice ports at system startup.

The voicecap values can be entered in a DSP-recognizable format called raw format. They can also be entered in standard format, which allows you to use commonly accessible values, such as decibels.

Starting with Cisco IOS Release 12.4(4)XC, this command can be used to configure GSMAMR-NB codecs on Cisco AS5350XM and Cisco AS5400XM platforms. The register values for GSMAMR-NB are shown in Table 245.

Table 245 GSMAMR-NB Register Values

V-Reg #	Default	Description	Register Values and Additional Notes
0	0	Sets how Adaptive Multi-Rate (AMR) responds to an incoming codec mode request (CMR) that is not a member of the mode set.	0 = Drop the packet with the bad CMR. 1 = Ignore the CMR (do not change rates) but process the rest of the packet data normally. 2 = Change the rate to the highest rate in the mode set lower than the rate requested by the CMR.
1	0	Sets how AMR handles packets with a frame type (AMR rate) that is not a member of the mode set.	0 = Drop the packet with the bad frame-type. 1 = Attempt to decode the packet.

Examples

The following example creates a voicecap string for a GSMAMR-NB codec named gsmamrnb-ctrl with V register 0 set to 1:

```
Router> enable
Router# configure terminal
Router(config)# voicecap entry gsmamrnb-ctrl v0=1
```

Related Commands

Command	Description
voicecap configure	Applies a voicecap to the specified voice ports.

voice call capacity mir

To set the value for the minimum interval between reporting (MIR), use the **voice call capacity mir** command in global configuration mode. To turn off these attributes, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity mir** *seconds*

no voice call {**carrier** | **trunk-group** | **prefix**} **capacity mir**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
seconds	Minimum interval, in seconds, with a range of 1 to 3600 seconds and a default of 10. This value cannot be set higher than the time configured for the **capacity update interval**.

Command Default

10 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Because the available circuit (AC) attribute of a destination is very dynamic, reporting of this attribute should be handled carefully. AC should be reported as frequently as possible so that the location server has better information about the resources. However, the location server should not be overwhelmed with too many updates.

All of the AC reporting, called the *interesting point of AC*, is performed when the specified event happens within the *minimum interval between reporting* (MIR) time since last reporting. This command sets the amount of time used for the interval to control the number of interesting points that are reported so not to overwhelm the location server with too many AC updates.

The *seconds* argument cannot be set higher than the time configured for the **capacity update interval**.

Examples

The following example shows the minimum interval between reporting for the carrier address family set to 25 seconds:

```
Router(config)# voice call carrier capacity mir 25
```

Related Commands

Command	Description
capacity update interval (dial peer)	Changes the capacity update for prefixes associated with a dial peer.
capacity update interval (trunk group)	Change the capacity update for carriers or trunk groups.
voice call capacity stw	Set the value for STW.

voice call capacity reporting

To turn on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity, use the **voice call capacity reporting** command in global configuration mode. To turn off the reporting, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity reporting** {**maxima** | **inflection**}

no voice call {**carrier** | **trunk-group** | **prefix**} **capacity reporting** {**maxima** | **inflection**}

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
maxima	Maxima (first derivative) point in available capacity.
inflection	Inflection (second derivative) point in available capacity.

Defaults

The capacity reporting function is turned off.

Command Modes

Global configuration.

Command History

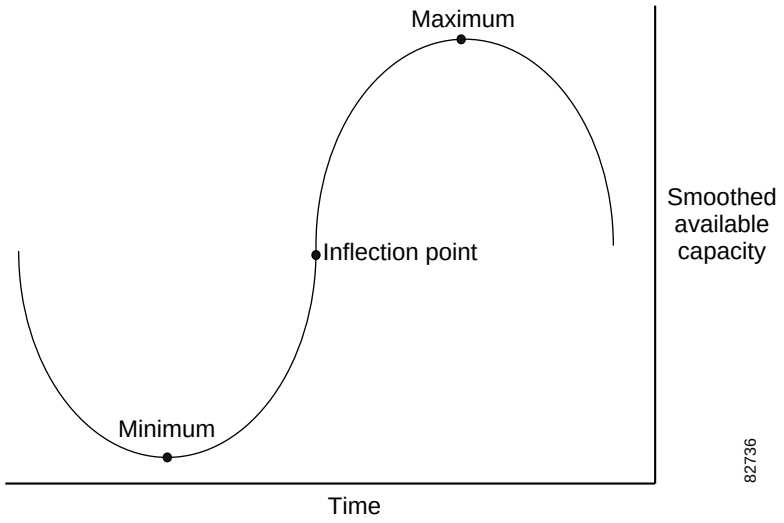
Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The smoothed curve of the available circuits (AC) has maxima, minima, and inflection points. When the curve has reached these points, this represents a change in the call rate.

Maximum, minimum and inflection points are illustrated in Figure 7.

Figure 7 Maximum, Minimum, and Inflection Points for Available Capacity



Examples

The following example shows the reporting of the available capacity inflection point on the trunk group is turned on:

```
Router(config)# voice call trunk-group capacity reporting inflection
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases
voice call trigger hwm	Sets the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases.

voice call capacity stw

To set the value for smoothing transition time for weight (STW), use the **voice call capacity stw** command in global configuration mode. To turn off these attributes, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity stw** *seconds*

no voice call {**carrier** | **trunk-group** | **prefix**} **capacity stw** *seconds*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
seconds	Transitions time can be from 0 to 60 seconds with a default of 10.

Command Default

10 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Because the available circuit (AC) attribute of a destination is very dynamic, reporting of this attribute should be handled carefully. AC should be reported as frequently as possible so that the location server has better information about the resources. However, the location server should not be overwhelmed with too many updates.

A smoothing algorithm is applied to the quantity of AC being reported. This algorithm eliminates reporting of noise. The degree of smoothing can be configured with the **voice call capacity stw** command. This command sets the smoothing transition time for weight, which is the time it takes for current smoothed value of AC to come half way between the current smoothed value and the current instantaneous value of AC. Lower **stw** values speed the smoothed value of AC as it approaches the instantaneous value of AC. When **stw** is set to 0, the smoothed value is always equal to the instantaneous value of AC.

Examples

The following example shows the smoothing time for weight for the carrier address family set to 25 seconds:

```
Router(config)# voice call carrier capacity stw 25
```

Related Commands

Command	Description
capacity update interval (dial peer)	Changes the capacity update for prefixes associated with a dial peer.
capacity update interval (trunk group)	Change the capacity update for carriers or trunk groups.
voice call capacity mir	Set the value for MIR.

voice call capacity timer interval

To set the periodic interval for reporting capacity from carrier, trunk group, or prefix databases, use the **voice call capacity timer interval** command in global configuration mode. To turn off the interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity timer interval** *seconds*

no voice call {**carrier** | **trunk-group** | **prefix**} **capacity timer interval** *seconds*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
seconds	Value from 10 to 3600 seconds.

Command Default 25 seconds

Command Modes Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines For the reporting interval, a periodic timer called the capacity update timer handles updates of available circuit (AC) information and can be configured using the **voice call capacity timer interval** command. For example, if AC has changed since the last reporting, the AC is again reported when the capacity update timer expires.

Examples The following example sets the timer interval for the prefixes set at 15 seconds:

```
Router(config)# voice call prefix capacity timer interval 15
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the MIR and STW.
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call trigger hwm	Sets the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases.

voice call convert-discpi-to-prog

To convert a disconnect message with a progress indicator (PI) to a progress message, use the **voice call convert-discpi-to-prog** command in global configuration mode. To return to the default condition, use the **no** form of this command.

voice call convert-discpi-to-prog [**tunnel-IEs** | **always** [**tunnel-IEs**]]

no voice call convert-discpi-to-prog

Syntax Description

tunnel-IEs	(Optional) Information elements (IEs) are carried in the progress message.
always	(Optional) Converts disconnect message with a PI to a progress message in both preconnected and connected states.

Command Default

A disconnect message with a PI is not converted to a progress message.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.
12.3(6)	The **tunnel-1Es** keyword was added.
12.3(4)XQ	The **always** keyword with the **tunnel-IEs keyword** were added.
12.3(8)T	The **always** keyword with the **tunnel-IEs keyword** were added.
12.3(9)	The **always** keyword with the **tunnel-1Es keyword** were added.

Usage Guidelines

The **voice call convert-discpi-to-prog** command turns an ISDN disconnect message into a progress message. If you use the **tunnel-IEs** keyword, the information elements are not dropped when the disconnect message is converted to a progress message.

Examples

The following example changes a disconnect with PI to a progress message containing information elements (IEs):

```
voice call convert-discpi-to-prog tunnel-IEs
```

The following example changes a disconnect with PI to a progress message in the preconnected and connected states:

```
voice call convert-discpi-to-prog always
```

Related Commands

Command	Description
disc_pi_off	Enables an H.323 gateway to disconnect a call when it receives a disconnect message with a PI.

voice call csr data-points

To set the number of call success rate (CSR) data points, use the **voice call csr data-points** command in global configuration mode. To disable the setting of the CSR data points, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr data-points** *value*

no voice call {**carrier** | **trunk-group** | **prefix**} **csr data-points** *value*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
value	Value from 10 to 50 data points. Default is 30 data points.

Command Default 30 data points

Command Modes Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples The following example sets the CSR data points for trunk groups at 10:

```
Router(config)# voice call trunk-group csr data-points 10
```

Related Commands

Command	Description
voice call csr recording interval	Sets the recording interval for CSR.
voice call csr reporting interval	Sets the reporting interval for CSR.

voice call csr recording interval

To set the recording interval for call success rates (CSR), use the **voice call csr recording interval** command in global configuration mode. To disable the CSR recording interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr recording interval** *minutes*

no voice call {**carrier** | **trunk-group** | **prefix**} **csr recording interval** *minutes*

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
minutes	Value from 10 to 1000 minutes with a default of 60.

Command Default

60 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example sets the CSR recording interval for prefixes at 30 minutes:

```
Router(config)# voice call carrier csr recording interval 30
```

Related Commands

Command	Description
voice call csr data-points	Sets the number of call success rate (CSR) data points.
voice call csr reporting interval	Sets the reporting interval for CSR.

voice call csr reporting interval

To set the reporting interval for call success rate (CSR), use the **voice call csr reporting interval** command in global configuration mode. To disable the CSR recording interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr reporting interval** *seconds*

no voice call {**carrier** | **trunk-group** | **prefix**} **csr reporting interval** *seconds*

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
seconds	Value from 10 to 10000 seconds with a default of 25.

Command Default

25 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example sets the CSR reporting interval for trunk groups at 40 seconds:

```
Router(config)# voice call carrier csr reporting interval 40
```

Related Commands

Command	Description
voice call csr data-points	Sets the number of CSR data points.
voice call csr recording interval	Sets the recording interval for CSR.

voice call debug

To debug a voice call, use the **voice call debug** command in global configuration mode. To display a full globally unique identifier (GUID) or header as explained in the Usage Guidelines section, use the **no** form of this command.

voice call debug full-guid | short-header

no voice call debug full-guid | short-header

Syntax Description

full-guid	Displays the GUID in a 16-byte header. **Note** When the **no** version of this command is input with the **full-guid** keyword, the short 6-byte version displays. This is the default.
short-header	Displays the CallEntry ID in the header without displaying the GUID or module-specific parameters.

Command Default

The short 6-byte header displays.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	The new debug header was added to the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850, and Cisco MC3810.
12.2(15)T	The header-only argument was removed and the short-header argument was added.

Usage Guidelines

Despite its nontraditional syntax (trailing rather than preceding “debug”), this is a normal **debug** command.

You can control the contents of the standardized header. Display options for the header are as follows:

- Short 6-byte GUID
- Full 16-byte GUID
- Short header which contains only the CallEntry ID

The format of the GUID headers is as follows:
//CallEntryID/GUID/Module-Dependent-List/Function-name:.

The format of the short header is as follows:
//CallEntryID/Function-name:.

When the **voice call debug short-header** command is entered, the header displays with no GUID or module-specific parameters. When the **no voice call debug short-header** command is entered, the header, the 6-byte GUID, and module-dependent parameter output displays. The default option is displaying the 6-byte GUID trace.

Note Using the **no** form of this command does not turn off debugging.

Examples

The following is sample output when the **full-guid** keyword is specified:

```
Router# voice call debug full-guid
!
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_insert_cdb:
00:05:12: //-1/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/CCAPI/cc_incr_if_call_volume:
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_open_voice_and
_set_params:
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_modem_proto_fr
om_cdb:
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/set_playout_cdb:
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_dsp_echo_cance
ller_control:
```

Note The "//-1/" output indicates that CallEntryID for the CCAPI module is not available.

Table 246 describes significant fields shown in the display.

Table 246 voice call debug full-guid Field Descriptions

Field	Description
VTSP:(0:D):0:0:4385	VTSP module, port name, channel number, DSP slot, and DSP channel number.
vtsp_insert_cdb	Function name.
CCAPI	CCAPI module.

The following is sample output when the **short-header** keyword is specified:

```
Router(config)# voice call debug short-header
!
00:05:12: //1/vtsp_insert_cdb:
00:05:12: //-1/cc_incr_if_call_volume:
00:05:12: //1/vtsp_open_voice_and_set_params:
00:05:12: //1/vtsp_modem_proto_from_cdb:
00:05:12: //1/set_playout_cdb:
00:05:12: //1/vtsp_dsp_echo_canceller_control:
```

Note The "//-1/" output indicates that CallEntryID for CCAPI is not available.

Related Commands

Command	Description
debug rtsp api	Displays debug output for the RTSP client API.
debug rtsp client session	Displays debug output for the RTSP client data.
debug rtsp error	Displays error message for RTSP data.
debug rtsp pmh	Displays debug messages for the PMH.
debug rtsp socket	Displays debug output for the RTSP client socket data.
debug voip ccapi error	Traces error logs in the CCAPI.
debug voip ccapi inout	Traces the execution path through the CCAPI.
debug voip ivr all	Displays all IVR messages.
debug voip ivr applib	Displays IVR API libraries being processed.
debug voip ivr callsetup	Displays IVR call setup being processed.
debug voip ivr digitcollect	Displays IVR digits collected during the call.
debug voip ivr dynamic	Displays IVR dynamic prompt play debug.
debug voip ivr error	Displays IVR errors.
debug voip ivr script	Displays IVR script debug.
debug voip ivr settlement	Displays IVR settlement activities.
debug voip ivr states	Displays IVR states.
debug voip ivr tclcommands	Displays the TCL commands used in the script.
debug voip rawmsg	Displays the raw VoIP message.
debug vtsp all	Enables **debug vtsp session**, **debug vtsp error**, and **debug vtsp dsp**.
debug vtsp dsp	Displays messages from the DSP.
debug vtsp error	Displays processing errors in the VTSP.
debug vtsp event	Displays the state of the gateway and the call events.
debug vtsp port	Limits VTSP debug output to a specific voice port.
debug vtsp rtp	Displays the voice telephony RTP packet debugging.
debug vtsp send-nse	Triggers the VTSP software module to send a triple redundant NSE.
debug vtsp session	Traces how the router interacts with the DSP.
debug vtsp stats	Debugs periodic statistical information sent and received from the DSP
debug vtsp vofr subframe	Displays the first 10 bytes of selected VoFR subframes for the interface.
debug vtsp tone	Displays the types of tones generated by the VoIP gateway.

voice call disc-pi-off

To enable the gateway to treat a disconnect message with progress indicator (PI) like a standard disconnect without a PI, use the **voice call disc-pi-off** command in global configuration mode. To reset to the default, use the **no** form of this command.

voice call disc-pi-off

no voice call disc-pi-off

Syntax Description

This command has no keywords or arguments.

Command Default

Gateway disconnects incoming call leg when it receives a disconnect message with PI.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command if the gateway is connected to a switch that sends a release immediately after it receives a Disconnect with PI. To properly handle the call, the switch should open a backward voice path and keep the call active. Otherwise the rotary dial peer feature does not work because the incoming call leg is disconnected. Using this command enables the gateway to handle a disconnect with PI like a regular disconnect message so that you can use the rotary dial peer feature.

Examples

The following example enables the gateway to properly handle a disconnect with PI:

```
voice call disc-pi-off
```

Related Commands

Command	Description
disc_pi_off	Enables an H.323 gateway to disconnect a call when it receives a disconnect message with a PI.
voice call convert-discpi-to-prog	Converts a disconnect message with a PI to a progress message.

voice call send-alert

To enable the terminating gateway to send an alert message instead of a progress message after it receives a call setup message, use the **voice call send-alert** command in global configuration mode. To reset to the default, use the **no** form of this command.

voice call send-alert

no voice call send-alert

Syntax Description

This command has no arguments or keywords.

Command Default

The terminating gateway sends a progress message after it receives a call Setup message.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI4	This command was introduced.
12.1(5)T	This command was not supported in this release.
12.1(5.3)T	This command was integrated into Cisco IOS Release 12.1(5.3)T.
12.2(1)	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later, the terminating gateway sends a Progress message with a progress indicator (PI) after it receives a Setup message. Previously, the gateway responded with an Alert message after receiving a call. In some cases, if the terminating switch does not forward the progress message to the originating gateway, the originating gateway does not cut-through the voice path until a Connect is received and the caller does not hear a ringback tone. In these cases, you can use the **voice call send-alert** command to make the gateway backward compatible with releases earlier than Cisco IOS Release 12.1(3)XI. If you configure the **voice call send-alert** command, the terminating gateway sends an Alert message after it receives a Setup message from the originating gateway.

To complete calls from a PRI to an FXS interface, configure the **voice call send-alert** command on the FXS device.

Examples

The following example configures the gateway to send an Alert message:

```
voice call send-alert
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

voice call trap deviation

To configure the percentage deviation for voice call trap parameters, use the **voice call trap deviation** command in global configuration mode. To disable the configured percentage deviation, use the **no** form of this command.

voice call trap deviation *percent* [**vad**]

no voice call trap deviation *percent* [**vad**]

Syntax Description

percent	The percentage deviation for trapping calls. The range of acceptable values is 1 to 100. The default is 49.
vad	(Optional) Specifies the deviation for calls with voice activity detection (VAD) turned on.

Command Default This command is enabled by default, and the deviation for trapping calls is set to 49 percent.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(12)	This command was introduced in a release earlier than Cisco IOS Release 12.4(12).
15.0(1)M	The **no** form of this command was modified.

Usage Guidelines Prior to Release 15.0(1)M, if a non-default *percent* value was configured, it could be disabled by entering the **no voice call trap deviation** *percent* command, even if the *percent* value was not the configured value. For example, if the **voice call trap deviation 30** command was configured, the **no voice call trap deviation 40** command disabled the initial command.

Beginning in Release 15.0(1)M, the *percent* value in the **no** form of the command must match the configured non-default value. For example, if the **voice call trap deviation 30** command is configured, the only way to disable it is to enter the **no voice call trap deviation 30** command. If the **no voice call trap deviation 40** command is entered, the command-line interface displays this message: "Please enter correct deviation."

Examples The following example shows how to set the deviation value for trapping calls to 30 percent:

```
Router(config)# voice call trap deviation 30 vad
```

voice call trigger hwm

To set the value for high water mark in the available capacity in the trunk group or prefix databases, use the **voice call trigger hwm** command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger hwm** *percent*

no voice call {**carrier** | **trunk-group** | **prefix**} **trigger hwm** *percent*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	Value can be 50 to 100 percent with a default of 80. If set to 100, this trigger will be turned off.

Command Default

80 percent

Command Modes

Global configuration.

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the value of AC goes above a threshold, called the *high water mark*. This can be configured with the **voice call trigger hwm** command. When the **hwm** option is selected and the value is set to 100, no update is sent due to high water mark.

Examples

The following example sets the trigger for available capacity on trunk groups to send at a high water mark of 75%:

```
Router(config)# voice call trunk-group trigger hwm 75
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases

Command	Description
voice call trigger lwm	Sets the value for low water mark in the available capacity for carrier, trunk group, or prefix databases
voice call trigger percent-change	Sets the value for percentage change in the available capacity for carrier, trunk group, or prefix databases

voice call trigger lwm

To set the value for low water mark in the available capacity in the trunk group or prefix databases, use the **voice call trigger lwm** command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger lwm** *percent*

no voice call {**carrier** | **trunk-group** | **prefix**} **trigger lwm** *percent*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	Value can be 0 to 30 percent with a default of 10. If set to 0, this trigger will be turned off.

Command Default

10 percent

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the value of AC falls below a threshold, called the *low water mark*. When the **lwm** option is selected and the value is set to 0, no update is sent due to low water mark.

Examples

The following example sets the trigger for available capacity for E.164 prefixes to send at a low water mark of 25%:

```
Router(config)# voice call prefix trigger lwm 25
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases.

Command	Description
voice call trigger hwm	Sets the value for high water mark in the available capacity for carrier, trunk group, or prefix databases
voice call trigger percent-change	Sets the value for percentage change in the available capacity for carrier, trunk group, or prefix databases

voice call trigger percent-change

To set the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases, use the **voice call trigger** command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger percent-change** *percent*

no voice call {**carrier** | **trunk-group** | **prefix**} **trigger percent-change** *percent*

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	If **percent-change** is selected, value can be 0 to 100 percent with a default of 30. If set to 0, this trigger will be turned off. If **lwm** is selected, value can be 0 to 30 percent with a default of 10. If set to 0, this trigger will be turned off. If **hwm** is select, value can be 50 to 100 percent with a default of 80. If set to 100, this trigger will be turned off.

Command Default

30 percent

Command Modes

Global configuration.

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the absolute percent change is above a threshold. When the **percent-change** option is selected and the value is set to 0, no update for percent change is sent

Examples

The following example sets the trigger for available capacity on the carrier codes to send at a percentage change of 15%:

```
Router(config)# voice call carrier trigger percent-change 15
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases
voice call trigger hwm	Sets the value for high water mark in the available capacity for carrier, trunk group, or prefix databases
voice call trigger lwm	Sets the value for low water mark in the available capacity for carrier, trunk group, or prefix databases

voice-card

To enter voice-card configuration mode and configure a voice card, use the **voice-card** command in global configuration mode. There is no **no** form of this command.

voice-card *slot*

Syntax Description

slot	Slot number for the card to be configured. The following platform-specific numbering schemes apply: • Cisco 2600 series and Cisco 2600XM: – 0 is the Advanced Integration Module (AIM) slot in the router chassis. – 1 is the network module slot in the router chassis. • Cisco 3600 series: – A value from 1 to 6 identifies a network module slot in the router chassis. • Cisco 3660: – 7 is AIM slot 0 in the router chassis. – 8 is AIM slot 1.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(5)XK	The command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)XB	Values for the *slot* argument were updated to include AIMs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T and implemented on the Cisco 1700 series, Cisco 2600XM, Cisco 3700 series, Cisco 7200 series, Cisco 7500 series, Cisco ICS7750, Cisco MC3810, and Cisco VG200.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines Voice-card configuration mode is used for commands that configure the use of digital signal processing (DSP) resources, such as codec complexity and DSPs. DSP resources can be found in digital T1/E1 packet voice trunk network modules on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.

Codec complexity is configured in voice-card configuration mode and has the following platform-specific usage guidelines:

- On Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745, the *slot* argument corresponds to the physical chassis slot of the network module that has DSP resources to be configured.

DSP resource sharing is also configured in voice-card configuration mode. On the Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745 under specific circumstances, configuration of the **dspfarm** command enters DSP resources on a network module or AIM into a DSP resource pool. Those DSP resources are then available to process voice traffic on a different network module or voice/WAN interface card (VWIC). See the **dspfarm (voice-card)** command reference for more information about DSP resource sharing.

Note When running high-complexity images, the system can only process up to 16 voice channels. Those 16 time slots need to be within a contiguous range (timeslot maximum (TSmax) minus timeslot minimum (TSmin) is less than or equal to 16, where TSmax and TSmin are the maximum DS0 and minimum DS0 configured for voice).

This command does not have a **no** form.

Examples

The following example enters voice-card configuration mode to configure resources on the network module in slot 1:

```
voice-card 1
```

The following example shows how to enter voice-card configuration mode and load high-complexity DSP firmware on voice-card 0. The **dspfarm** command enters the DSP resources on the AIM specified in the **voice-card** command into the DSP resource pool.

```
voice-card 0
 codec complexity high
 dspfarm
```

Related Commands

Command	Description
codec complexity	Matches the DSP complexity packaging to the codecs to be supported.
dspfarm (voice-card)	Adds the specified voice card to those participating in a DSP resource pool.

voice cause-code

To set the internal Q850 cause code mapping for voice and to enter voice cause configuration mode, use the **voice cause-code** command in global configuration mode. To disable the internal Q850 cause code mapping for voice, use the **no** form of this command.

voice cause-code

no voice cause-code

Syntax Description

This command has no arguments or keywords.

Command Default

Internal Q850 cause code mapping for voice is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to set the cause code mapping for voice:

```
Router> enable
Router# configure terminal
Router(config)# voice cause-code
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class aaa

To enable dial-peer-based VoIP AAA configurations, use the **voice class aaa** command in global configuration mode. To disable dial-peer-based VoIP AAA configurations, use the **no** form of this command.

voice class aaa *tag*

no voice class aaa *tag*

Syntax Description

tag	A number used to identify voice class AAA. The range is from 1 to 10000. There is no default value.

Command Default No default behaviors or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines The **voice class aaa** configuration command sets up a voice service class that allows you to perform dial-peer-based AAA configurations.

The command activates voice class AAA configuration mode. Commands that are configured in voice class AAA configuration mode are listed in the "Related Commands" section.

Examples The following example shows AAA configurations in voice class AAA configuration mode. The number assigned to the tag is 1.

```
voice class aaa 1
 authentication method dp
 authorization method dp
 accounting method dp
in-bound
 accounting template temp-dp
```

The following example shows accounting configurations in voice class AAA configuration mode:

```
voice class aaa 2
 accounting method dp-out out-bound
 accounting template temp-dp out-bound
```

Related Commands

Command	Description
authentication method	Specifies an authentication method for calls coming into the defined dial peer.
authorization method	Specifies an authorization method for calls coming into the defined dial peer.
method	Specifies an accounting method for calls coming into the defined dial peer.
accounting suppress	Disables accounting that is automatically generated by the service provider module for a specific dial peer.
voice-class aaa	Applies properties defined in the voice class to a specific dial peer.

voice class busyout

To create a voice class for local voice busyout functions, use the **voice class busyout** command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class busyout *tag*

no voice class busyout *tag*

Syntax Description

tag	Unique identification number assigned to one voice class. Range is 1 to 10000.

Command Default

No voice class is configured for busyout functions.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

You can apply a busyout voice class to multiple voice ports. You can assign only one busyout voice class to a voice port. If a second busyout voice class is assigned to a voice port, the second voice class replaces the one previously assigned.

If you assign a busyout voice class to a voice port, you may not assign separate busyout commands directly to the voice port, such as **busyout monitor serial**, **busyout monitor ethernet**, or **busyout monitor probe**.

Examples

The following example configures busyout voice class 20, in which the connections to two remote interfaces are monitored by a response time reporter (RTR) probe with a G.711ulaw profile, and voice ports are busied out whenever both links have a packet loss exceeding 10 percent and a packet delay time exceeding 2 seconds:

```
voice class busyout 20
 busyout monitor probe 171.165.202.128 g711u loss 10 delay 2000
 busyout monitor probe 171.165.202.129 g711u loss 10 delay 2000
```

The following example configures busyout voice class 30, in which voice ports are busied out when serial ports 0/0, 1/0, 2/0, and 3/0 go out of service.

```
voice class busyout 30
 busyout monitor serial 0/0
 busyout monitor serial 1/0
 busyout monitor serial 2/0
 busyout monitor serial 3/0
```

Related Commands

Command	Description
busyout monitor ethernet	Configures a voice port to monitor a local Ethernet interface for events that would trigger a voice-port busyout.
busyout monitor probe	Configures a voice port to enter the busyout state if an RTR probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
busyout monitor serial	Configures a voice port to monitor a serial interface for events that would trigger a voice-port busyout.
show voice busyout	Displays information about the voice busyout state.

voice class called number

To define a voice class called number or range of numbers, use the **voice class called number** command in global configuration mode. To remove a voice class called number, use the **no** form of this command.

voice class called number {**inbound** | **outbound** | **pool**} *tag*

no voice class called number

Syntax Description

inbound	Inbound voice class called number.
outbound	Outbound voice class called number.
pool	Voice class called number pool.
tag	Digits that identify a specific inbound or outbound voice class called number or voice class called number pool.

Command Default No voice class called number is configured.

Command Modes Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to define one or more static voice class called numbers for inbound and outbound POTS dial peers or a dynamic voice class called number pool. The indexes for a voice class called number are defined with the **index** (voice class) command.

Note Enter the **voice class called number** command in global configuration mode without hyphens. Enter the **voice-class called-number** command in dial peer configuration mode with hyphens.

Examples The following example shows configuration for an outbound voice class called number:

```
voice class called number outbound 30
 index 1 5550100
 index 2 5550101
 index 3 5550102
 index 4 5550103
```

The following example shows configuration for a voice class called number pool:

```
voice class called number pool 1
 index 1 5550100 - 5550199
```

Related Commands

Command	Description
show voice class called-number	Displays a specific voice class called number.
voice-class called-number (dial peer)	Assigns a previously defined voice class called number to an inbound or outbound POTS dial peer.

voice class cause-code

To configure cause code list parameters for a voice class and to enter cause code configuration mode, use the **voice class cause-code** command in global configuration mode. To disable the cause code list parameters configuration for a voice class, use the **no** form of this command.

voice class cause-code *number*

no voice class cause-code *number*

Syntax Description

number	Numeric tag that specifies the voice class cause code. The range is from 1 to 64.

Command Default

The cause code list parameters are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure cause code list parameters for voice class 5:

```
Router> enable
Router# configure terminal
Router(config)# voice class cause-code 5
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class codec

To enter voice-class configuration mode and assign an identification tag number for a codec voice class, use the **voice class codec** command in global configuration mode. To delete a codec voice class, use the **no** form of this command.

voice class codec *tag*

no voice class codec *tag*

Syntax Description

tag	Unique number that you assign to the voice class. Range is from 1 to 10000. There is no default.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300.
12.0(7)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command only creates the voice class for codec selection preference and assigns an identification tag. Use the **codec preference** command to specify the parameters of the voice class, and use the **voice-class codec** dial-peer command to apply the voice class to a VoIP dial peer.

Note The **voice class codec** command in global configuration mode is entered without a hyphen. The **voice-class codec** command in dial peer configuration mode is entered with a hyphen.

Examples

The following example shows how to enter voice-class configuration mode and assign a voice class tag number starting from global configuration mode:

```
voice class codec 10
```

After you enter voice-class configuration mode for codecs, use the **codec preference** command to specify the parameters of the voice class.

The following example creates preference list 99, which can be applied to any dial peer:

```
voice class codec 99
 codec preference 1 g711alaw
 codec preference 2 g711ulaw bytes 80
 codec preference 3 g723ar53
```

```
codec preference 4 g723ar63 bytes 144
codec preference 5 g723r53
codec preference 6 g723r63 bytes 120
codec preference 7 g726r16
codec preference 8 g726r24
codec preference 9 g726r32 bytes 80
codec preference 10 g728
codec preference 11 g729br8
codec preference 12 g729r8 bytes 50
```

Related Commands

Command	Description
codec preference	Specifies a list of preferred codecs to use on a dial peer.
test voice port detector	Defines the order of preference in which network dial peers select codecs.
voice-class codec (dial peer)	Assigns a previously configured codec selection preference list to a dial peer.

voice class custom-cptone

To create a voice class for defining custom call-progress tones to be detected, use the **voice class custom-cptone command in** global configuration mode. To delete the voice class, use the **no** form of this command.

voice class custom-cptone *cptone-name*

no voice class custom-cptone *cptone-name*

Syntax Description

cptone-name	Descriptive identifier for this class of custom call-progress tones that associates this set of custom call-progress tones with voice ports.

Command Default

No voice class of custom call-progress tones is created.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810 platforms.
12.2(2)T	This command was implemented on Cisco 1750 access routers and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

After you create a voice class, you need to define custom call-progress tones for this voice class using the **dualtone** command.

Examples

The following example creates a voice class named country-x.

```
voice class custom-cptone country-x
```

The following example deletes the voice class named country-x.

```
no voice class custom-cptone country-x
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class dualtone-detect-params	Modifies the boundaries and limits for call-progress tones.

voice class dualtone

To create a voice class for Foreign Exchange Office (FXO) supervisory disconnect tone detection parameters, use the **voice class dualtone** command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class dualtone *tag*

no voice class dualtone *tag*

Syntax Description

tag	Unique identification number assigned to one voice class. Range is from 1 to 10000.

Command Default No voice class is configured for tone detection parameters.

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600, and the Cisco MC3810.

Usage Guidelines Use this command first to create the voice class. Then use the **supervisory disconnect dualtone voice-class** command to assign the voice class to a voice port.

A voice class can define any number of tones to be detected. You need to define a matching tone for each supervisory disconnect tone expected from a PBX or from the public switched telephone network (PSTN).

Examples The following example configures voice class dualtone 70, which defines one tone with two frequency components, and does not configure a cadence list:

```
voice class dualtone 100
 freq-pair 1 350 440
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
 cadence-min-on-time 50
 cadence-max-off-time 400
 cadence-variation 8
 exit
```

The following example configures voice class dualtone 100, which defines one tone with two frequency components, and configures a cadence list:

```
voice class dualtone 100
```

```
 freq-pair 1 350 440
 freq-pair 2 480 850
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
 cadence-min-on-time 50
 cadence-max-off-time 400
 cadence-list 1 100 100 300 300
 cadence-variation 8
 exit
```

The following example configures voice class dualtone 90, which defines three tones, each with two frequency components, and configures two cadence lists:

```
voice class dualtone 90
 freq-pair 1 350 440
 freq-pair 2 480 850
 freq-pair 3 1000 1250
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
 cadence-min-on-time 50
 cadence-max-off-time 500
 cadence-list 1 100 100 300 300 100 200
 cadence-list 2 100 200 100 400
 cadence-variation 8
 exit
```

Related Commands

Command	Description
supervisory disconnect dualtone voice-class	Assigns a previously configured voice class for FXO supervisory disconnect tone to a voice port.

voice class dualtone-detect-params

To create a voice class for defining a set of tolerance limits for the frequency, power, and cadence parameters of the tones to be detected, use the **voice class dualtone-detect-params** command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class dualtone-detect-params *tag*

no voice class dualtone-detect-params *tag*

Syntax Description

tag	Unique tag identification number assigned to a voice class. Range is from 1 to 10000.

Command Default No voice class is configured for defining answer-supervision tolerance limits.

Command Modes Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on Cisco 1750 routers and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines Use this command to create a voice class in which you can define maximum and minimum call-progress tone tolerance parameters that you can apply to any voice port. These parameters further define the call-progress tones defined by the **voice class custom-cptone** command. Use the **supervisory dualtone-detect-params** command to apply these tolerance parameters to a voice port.

Examples The following example creates voice class 70, in which you can specify modified boundaries and limits for call-progress tone detection.

```
voice class dualtone-detect-params 70
freq-max-deviation 25
freq-max-power -5
freq-min-power -20
freq-power-twist 10
freq-max-delay 50
cadence-variation 80
exit
```

Related Commands

Command	Description
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters defined by the **voice class dualtone-detect-params** command to a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

voice class h323

To create an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers, use the **voice class h323** command in global configuration mode. To remove the voice class, use the **no** form of this command.

voice class h323 *tag*

no voice class h323

Syntax Description

tag	Unique number to identify the voice class. Range is from 1 to 10000. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco AS5300, Cisco uBR910, and Cisco uBR924.

Usage Guidelines

The **voice class h323** command in global configuration mode does not include a hyphen. The **voice-class h323** command in dial peer configuration mode includes a hyphen.

Examples

The following example demonstrates how a voice class is created and applied to an individual dial peer. Voice class 4 contains a command to disable the capability to detect Cisco CallManager systems in the network (this command is used by Cisco CallManager Express 3.1 and later versions). The example then uses the **voice-class h323** command to apply voice class 4 to dial peer 36.

```
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.

voice class media

To configure the media control parameters for voice, use the **voice class media** command in global configuration mode. To disable the media control parameters for voice, use the **no** form of this command.

voice class media *number*

no voice class media *number*

Syntax Description

number	Numeric tag that specifies the voice class media. The range is from 1 to 10000.

Command Default The media control parameters for voice are not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples The following example shows how to configure media control parameters for voice:

```
Router> enable
Router# configure terminal
Router(config)# voice class media 5
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class permanent

To create a voice class for a Cisco trunk or FRF.11 trunk, use the **voice class permanent** command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class permanent *tag*

no voice class permanent *tag*

Syntax Description

tag	Unique number that you assign to the voice class. Range is from 1 to 10000.

Command Default No voice class is configured.

Command Modes Global configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines The **voice class permanent** command can be used for Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Voice over IP (VoIP) trunks.

The **voice class permanent** command in global configuration mode is entered without a hyphen. The **voice-class permanent** command in dial-peer and voice-port configuration modes is entered with a hyphen.

Examples The following example shows how to create a permanent voice class starting from global configuration mode:

```
voice class permanent 10
 signal keepalive 3
 exit
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type for a network dial peer.
voice-class permanent	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer.

voice class resource-group

To enter voice-class configuration mode and assign an identification tag number for a resource group, use the **voice class resource-group** command in global configuration mode. To delete a resource group, use the **no** form of this command.

voice class resource-group *tag*

no voice class resource-group *tag*

Syntax Description

tag	Unique tag to identify the resource. The range is from 1 to 5.

Command Default No resource groups are created.

Command Modes Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines Use the **voice class resource-group** command to configure parameters along with the threshold values to be monitored for resource groups. When you use the **voice class resource-group** command, the router enters voice-class configuration mode. You can then group the resources to be monitored and configure parameters such as .

Examples The following example shows how to enter voice-class configuration mode and assign identification tag number 5 for a resource group:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 5
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.

voice class sip-copylist

To configure a list of entities to be sent to the peer call leg, use the **voice class sip-copylist** command in global configuration mode. To disable the configuration, use the **no** form of this command.

voice class sip-copylist *tag*

no voice class sip-copylist *tag*

Syntax Description

tag	Voice class Session Initiation Protocol (SIP) copylist tag. The range is from 1 to 10000.

Command Default

No header is sent to the peer call leg.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **voice class sip-copylist** command to configure Cisco Unified Border Element (UBE) to pass an unsupported parameter present in a mandatory header from one call leg to another of Cisco UBE. You can copy the inbound message headers into variables and pass the headers to the outbound call leg.

Examples

The following example shows how to configure a SIP list to be sent to the peer call leg:

```
Router(config)# voice class sip-copylist 5
```

Related Commands

Command	Description
sip-header	Specifies the SIP header to be sent to the peer call leg.

voice class sip-profiles

To configure Session Initiation Protocol (SIP) profiles for a voice class, use the **voice class sip-profiles** command in global configuration mode. To disable the SIP profiles for a voice class, use the **no** form of this command.

voice class sip-profiles *number*

no voice class sip-profiles *number*

Syntax Description

number	Numeric tag that specifies the voice class SIP profile. The range is from 1 to 10000.

Command Default SIP profiles for a voice class are not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples The following example shows to specify SIP profile 2 for a voice class:

```
Router> enable
Router# configure terminal
Router(config)# voice class sip-profiles 2
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice-class stun-usage

To configure voice class, enter voice class configuration mode called stun-usage and use the **voice-class stun-usage** command in global, dial-peer, ephone, ephone template, voice register pool, or voice register pool template configuration mode. To disable the voice class, use the **no** form of this command.

voice-class stun-usage *tag*

no voice-class stun-usage *tag*

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

The voice class is not defined.

Command Modes

Global configuration (config)
Dial peer configuration (config-dial-peer)
Ephone configuration (config-ephone)
Ephone template configuration (config-ephone-template)
Voice register pool configuration (config-register-pool)
Voice register pool template configuration (config-register-pool)

Command History

Release	Cisco Product	Modification
12.4(22)T	Cisco Unified CME 7.0	This command was introduced.
15.1(2)T	Cisco Unified CME 8.1	This command was modified. This command can be enabled in ephone summary, ephone template, voice register pool, or voice register pool template configuration mode.

Usage Guidelines

When the voice-class stun-usage is removed, the same is removed automatically from the dial-peer, ephone, ephone template, voice register pool, or voice register pool template configurations.

Examples

The following example shows how to set the **voice class stun-usage** tag to 10000:

```
Router(config)# voice class stun-usage 10000
Router(config-ephone)# voice class stun-usage 10000
Router(config-voice-register-pool)# voice class stun-usage 10000
```

Related Commands

Command	Description
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
stun flowdata agent-id	Configures the agent ID.

voice class tone-signal

To enter voice-class configuration mode and create a tone-signal voice class, use the **voice class tone-signal** command in global configuration mode. To delete a tone-signal voice class, use the **no** form of this command.

voice class tone-signal *tag*

no voice class tone-signal *tag*

Syntax Description

tag	Label that uniquely identifies the voice class. Can be up to 32 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use the **voice class tone-signal** command to define wakeup, frequency selection, and guard tones to be played out before and during the voice packets for a specific voice port. Use the **inject guard-tone**, **inject pause**, and **inject tone** commands to define the tone signaling in this class. You can configure up to ten tones in a tone-signal voice class.

To avoid voice loss at the receiving end of an LMR system, the maximum of the sum of the durations of the injected tones and pauses in the voice class should not exceed 1500 milliseconds. You must also use the **timing delay-voice tdm** command to configure a delay for the voice packet equal to the sum of the durations of all the injected tones and pauses.

Note that the hyphenation in this command differs from the hyphenation used in a similar command, **voice-class tone-signal**, which is used in voice-port configuration mode.

Examples

The following example shows how to create a tone-signal voice class starting from global configuration mode:

```
voice class tone-signal mytones
 inject tone 1 1950 3 150
 inject tone 2 2000 0 60
 inject pause 3 60
 inject tone 4 2175 3 150
 inject tone 5 1000 0 50
```

Related Commands

Command	Description
inject guard-tone	Plays out a guard tone with the voice packet.
inject pause	Specifies a pause between injected tones.
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.
timing delay-voice tdm	Specifies the delay before a voice packet is played out.
voice-class tone-signal	Assigns a previously configured tone-signal voice class to a voice port.

voice class uri

To create or modify a voice class for matching dial peers to a Session Initiation Protocol (SIP) or telephone (TEL) uniform resource identifier (URI), use the **voice class uri** command in global configuration mode. To remove the voice class, use the **no** form of this command.

voice class uri *tag* {**sip** | **tel**}

no voice class uri *tag*

Syntax Description

tag	Label that uniquely identifies the voice class. Can be up to 32 alphanumeric characters.
sip	Voice class for SIP URIs.
tel	Voice class for TEL URIs.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- This command takes you to voice URI class configuration mode, where you configure the match characteristics for a URI. The commands that you enter in this mode define the set of rules by which the URI in a call is matched to a dial peer.
- To reference this voice class for incoming calls, use the **incoming uri** command in the inbound dial peer. To reference this voice class for outgoing calls, use the **destination uri** command in the outbound dial peer.
- Using the **no voice class uri** command removes the voice class from any dial peer where it is configured with the **destination uri** or **incoming uri** commands.

Examples The following example defines a voice class for SIP URIs:

```
voice class uri r100 sip
 user-id abc123
 host server1
 phone context 408
```

The following example defines a voice class for TEL URIs:

```
voice class uri r101 tel
 phone number ^408
 phone context 408
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
phone number	Matches a call based on the phone number field in a TEL URI.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.

voice class uri sip preference

To set the preference for selecting a voice class for Session Initiation Protocol (SIP) uniform resource identifiers (URIs), use the **voice class uri sip preference** command in global configuration mode. To reset to the default, use the **no** form of this command.

voice class uri sip preference {**user-id** | **host**}

no voice class uri sip preference

Syntax Description

user-id	User-id field is given preference.
host	Host field is given preference.

Command Default Host field

Command Modes Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command to resolve ties when more than one voice class is matched for a SIP URI. The default is to match on the host field of the URI.
- This command applies globally to all URI voice classes for SIP.

Examples The following example defines the preference as the user-id for a SIP voice class:

```
voice class uri sip preference user-id
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
user-id	Matches a call based on the user-id field in the SIP URI.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.

Command	Description
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.

voice-class aaa (dial peer)

To apply properties defined in the voice class to a dial peer, use the **voice-class aaa** command in dial peer configuration mode. This command does not have a **no** form.

voice-class aaa *tag*

Syntax Description

tag	A number to identify the voice class. Range is from 1 to 10000. There is no default.

Command Default No default behaviors or values

Command Modes Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines Properties that are configured in voice class AAA configuration mode can be applied to a dial peer by using this command.

Examples The following example shows redirecting AAA requests using Digital Number Identification Service (DNIS). You define a voice class to specify the AAA methods and then use this command.

```
voice class aaa 1
  authentication method kz
  authorization method kz
  accounting method kz
!
dial-peer voice 100 voip
  incoming called-number 50..
  session target ipv4:1.5.31.201
  voice-class aaa 1
```

Related Commands

Command	Description
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

voice-class called-number (dial peer)

To assign a previously defined voice class called number to an inbound or outbound POTS dial peer, use the **voice-class called-number** command in dial peer configuration mode. To remove a voice class called number from the dial peer, use the **no** form of this command.

voice-class called-number [**inbound** | **outbound**] *tag*

no voice-class called-number

Syntax Description

inbound	Assigns an inbound voice class called number to the dial peer.
outbound	Assigns an outbound voice class called number to the dial peer.
tag	Digits that identify a specific voice class called number.

Command Default No voice class called number is configured on the dial peer.

Command Modes Dial peer configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines Use this command to assign a previously defined voice class called number to a dial peer for a static H.320 secondary call dial plan. Use the **inbound** keyword for inbound POTS dial peers, and the **outbound** keyword for outbound POTS dial peers.

Note The **voice class called number** command in global configuration mode is entered without hyphens. The **voice-class called-number** command in dial peer configuration mode is entered with hyphens.

Examples The following example shows configuration for an outbound voice class called number outbound on POTS dial peer 22:

```
dial-peer voice 22 pots
 voice-class called-number inbound 300
```

Related Commands

Command	Description
voice class called number	Defines a voice class called number or range of numbers for H.320 calls.
voice-class called-number-pool	Defines a pool of dynamic voice class called numbers for a voice port.

voice-class called-number-pool

To assign a previously defined voice class called number pool to a voice port, use the **voice-class called-number-pool** command in voice class configuration mode. To remove a voice class called number pool from the voice port, use the **no** form of this command.

voice-class called-number-pool *tag*

no voice-class called-number-pool

Syntax Description

tag	Digits that identify a specific voice class called number pool.

Command Default

No voice class called number pool is assigned to the voice port.

Command Modes

Voice class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to assign a voice class called number pool to a voice port for a dynamic H.320 secondary call dial plan.

Examples

The following example shows configuration for voice class called number pool 100 on voice port 1/0/0:

```
voice-port 1/0/0
 voice-class called-number-pool 100
```

Related Commands

Command	Description
voice class called number	Defines a voice class called number or range of numbers for H.320 calls.
voice-class called-number (dial peer)	Defines a called number or range of called numbers for a POTS dial peer.

voice-class codec (dial peer)

To assign a previously configured codec selection preference list (codec voice class) to a VoIP dial peer, enter the **voice-class codec** command in dial-peer configuration mode. To remove the codec preference assignment from the dial peer, use the **no** form of this command.

voice-class codec *tag* [**offer-all**]

no voice-class codec

Syntax Description

tag	Unique number assigned to the voice class. The range is from 1 to 10000. • This tag number maps to the tag number created using the **voice class codec** command available in global configuration mode.
offer-all	(Optional) Adds all the configured codecs from the voice class codec to the outgoing offer from the Cisco Unified Border Element (Cisco UBE).

Command Default Dial peers have no codec voice class assigned.

Command Modes Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(2)XH	This command was introduced in Cisco IOS Release 12.0(2)XH and implemented on the Cisco AS5300 series routers.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T and implemented on the Cisco 2600 series and the Cisco 3600 series.
12.0(7)XK	This command was integrated into Cisco IOS Release 12.0(7)XK and implemented on the Cisco MC3810.
15.1(2)T	This command was modified. The **offer-all** keyword was added.

Usage Guidelines You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

Note The **voice-class codec** command in dial-peer configuration mode is entered with a hyphen. The **voice class codec** command in global configuration mode is entered without a hyphen.

Examples The following example shows how to assign a previously configured codec voice class to a dial peer:

```
Router# configure terminal
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# voice-class codec 10 offer-all
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all dial peers configured on the router.
test voice port detector	Defines the order of preference in which network dial peers select codecs.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.

voice-class h323 (dial peer)

To assign an H.323 voice class to a VoIP dial peer, use the **voice-class h323** command in dial peer configuration mode. To remove the voice class from the dial peer, use the **no** form of this command.

voice-class h323 *tag*

no voice-class h323 *tag*

Syntax Description

tag	Unique number to identify the voice class. Range is from 1 to 10000.

Command Default The dial peer does not use an H.323 voice class.

Command Modes Dial peer configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines The voice class that you assign to the dial peer must be configured using the **voice class h323** in global configuration mode.

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

The **voice-class h323** command in dial peer configuration mode includes a hyphen and in global configuration mode does not include a hyphen.

Examples The following example demonstrates how a voice class is created and applied to an individual dial peer. Voice class 4 contains a command to disable the capability to detect Cisco CallManager systems in the network (this command is used by Cisco CallManager Express 3.1 and later versions). The example then uses the **voice-class h323** command to apply voice class 4 to dial peer 36.

```
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7
Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all dial peers configured on the router.
voice class h323	Enters voice-class configuration mode and assigns an identification tag number for an H.323 voice class.

voice-class permanent (dial peer)

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer, use the **voice-class permanent** command in dial peer configuration mode. To remove the voice-class assignment from the network dial peer, use the **no** form of this command.

voice-class permanent *tag*

no voice-class permanent *tag*

Syntax Description

tag	Unique number assigned to the voice class. The *tag* number maps to the tag number created using the **voice class permanent** global configuration command. Range is from 1 to 10000.

Command Default Network dial peers have no voice class assigned.

Command Modes Dial peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines You can assign one voice class to any given network dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

You cannot assign a voice class to a plain old telephone service (POTS) dial peer.

The **voice-class permanent** command in dial peer configuration mode is entered with a hyphen. The **voice class permanent** command in global configuration mode is entered without a hyphen.

Examples The following example assigns a previously configured voice class to a Voice over Frame Relay (VoFR) network dial peer:

```
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type for a network dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

voice-class permanent (voice-port)

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a voice port, use the **voice-class permanent** command in voice-port configuration mode. To remove the voice-class assignment from the voice port, use the **no** form of this command.

voice-class permanent *tag*

no voice-class permanent *tag*

Syntax Description

tag	Unique number assigned to the voice class. The *tag* number maps to the tag number created using the **voice class permanent** global configuration command. Range is 1 to 10000.

Command Default Voice ports have no voice class assigned.

Command Modes Voice-port configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented as a voice-port configuration command on Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines You can assign one voice class to any given voice port. If you assign another voice class to a voice port, the last voice class assigned replaces the previous voice class.

The **voice-class permanent** command in voice-port configuration mode is entered with a hyphen. The **voice class permanent** command in global configuration mode is entered without a hyphen.

Examples The following example assigns a previously configured voice class to voice port 1/1/0:

```
voice-port 1/1/0
 voice-class permanent 10
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type for a network dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

voice-class sip anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip anat** command in SIP configuration or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

voice-class sip anat [**system**]

no voice-class sip anat [**system**]

Syntax Description

system	(Optional) Configures ANAT globally.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

SIP configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Both the Cisco IOS SIP gateway and Cisco Unified Border Element are required to support the Session Description Protocol (SDP) ANAT semantics. The **bind** command allows the use of ANAT semantics in outbound SDP. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IPv4 versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped “m” lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only mode or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

The **system** keyword configures ANAT on all network dial peers, including the local dial peer. Using the **voice-class sip anat** command without the **system** keyword enables ANAT only for the local dial peer.

Examples

The following example globally enables ANAT on a SIP trunk:

```
Router(config-serv-sip)# voice-class sip anat system
```

The following example enables ANAT on a specified dial peer:

```
Router(config-dial-peer)# voice-class sip anat
```

Related Commands

Command	Description
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

voice-class sip associate registered-number

To associate the preloaded route and outbound proxy details to the registered number in the dail peer configuration mode, use the **voice-class sip associate registered-number** command in dial peer configuration mode. To remove the association, use the **no** form of this command.

voice-class sip associate registered-number *number* [**system**]

no voice-class sip associate registered-number

Syntax Description

number	Registered number. The number must be between 4 and 32.
system	(Optional) Configures the association globally.

Command Default

The preloaded route and outbound proxy details are not associated by default.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **voice-class sip associate registered-number** command takes precedence over the **associate registered-number** command in voice service VOIP SIP configuration mode. However, if the **voice-class sip associate registered-number** command is used with the **system** keyword, the gateway uses the settings configured globally by the **associate registered-number** command.

Examples

The following example shows how to associate a registered number on dial peer.

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip associate registered-number 20
```

Related Commands

Command	Description
associate registered-number	Associates the preloaded route and outbound proxy details with the registered number in voice service VoIP SIP configuration mode.

voice-class sip asymmetric payload

To configure dynamic Session Initiation Protocol (SIP) asymmetric payload support on a dial peer, use the **voice-class sip asymmetric payload** command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip asymmetric payload {**dtmf** | **dynamic-codecs** | **full** | **system**}

no voice-class sip asymmetric payload

Syntax Description

dtmf	Provides asymmetric support only for dual-tone multi-frequency (DTMF) payloads.
dynamic-codecs	Provides asymmetric support only for dynamic codec payloads.
full	Provides asymmetric support both for DTMF and dynamic codec payloads.
system	(Optional) Specifies that the asymmetric payload uses the global value.

Command Default

Disabled (dynamic SIP asymmetric payload support is not enabled).

Command Modes

Dial peer (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS Release IOS XE 3.1S

Usage Guidelines

For the Cisco UBE the SIP asymmetric payload-type is supported for audio/video codecs, DTMF, and NSE. Hence, **dtmf** and **dynamic-codecs** keywords are internally mapped to the **full** keyword to provide asymmetric payload-type support for audio/video codecs , DTMF, and NSE.

Examples

The following example shows how to configure dynamic SIP asymmetric payload support:

```
Router# configure terminal
Router(config)# dial-peer voice 77 voip
Router(config-dial-peer)# voice-class sip asymmetric payload full
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice-class sip authenticate redirecting-number

To supersede global settings and enable a dial peer on a Cisco IOS voice gateway to authenticate and pass Session Initiation Protocol (SIP) credentials based on the redirecting number of forwarded calls, use the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode. To supersede global settings and specify that a dial peer uses only the calling number of forwarded calls, use the **no** form of this command. To return a dial peer to the default setting so that the dial peer uses the global setting, use the **default** form of this command.

voice-class sip authenticate redirecting-number [**system**]

no voice-class sip authenticate redirecting-number

default voice-class sip authenticate redirecting-number

Syntax Description

system	(Optional) Specifies that the dial peer use whatever setting is configured at the global (voice service SIP) command level (default).

Command Default

The dial peer uses the global setting. If the global setting is not specifically configured, the dial peer uses only the calling number of a forwarded call for SIP credentials even when the redirecting number is available for that call.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When an INVITE message sent out by the gateway is challenged, it must respond with the appropriate SIP credentials before the call is established. The default global behavior for the gateway is to authenticate and pass SIP credentials based on the calling number and all dial peers on a gateway default to the global setting. However, for forwarded calls, it is sometimes more appropriate to use the redirecting number and this can be specified at either the global or dial peer level (configuring behavior for a specific dial peer supersedes the global setting).

Use the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode to supersede global settings and enable a dial peer to authenticate and pass SIP credentials based on the redirecting number when available. Use the **no** form of this command to supersede global settings and force a dial peer to authenticate and pass SIP credentials based only on the calling number of forwarded calls. Use the **default** form of this command to configure the dial peer to use the global setting.

The redirecting number is present only in the headers of forwarded calls. When the **voice-class sip authenticate redirecting-number** command is disabled or the redirecting number is not available, the dial peer passes SIP credentials that are based on the calling number of the forwarded call. This is also the behavior on dial peers that are configured to use the global setting and the global setting is disabled (default). To enable the global setting (which is used as the default setting for all dial peers on the gateway), use the **authenticate redirecting-number** command in voice service SIP configuration mode.

Examples

The following example shows how to enable dial peer 2 to authenticate and pass SIP credentials based on the redirecting number (if available) of a forwarded call when a SIP INVITE message is challenged:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip authenticate redirecting-number
```

The following example shows how to force dial peer 2 to authenticate and pass only the calling number of a call even when the global setting is enabled and a redirecting number is available for a call:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# no voice-class sip authenticate redirecting-number
```

The following two examples show different ways of setting dial peer 2 to the default setting so that it authenticates and passes either the redirecting or calling number of a call based on the global (system) setting for the gateway:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# default voice-class sip authenticate redirecting-number

Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip authenticate redirecting-number system
```

Related Commands

Command	Description
authenticate redirecting-number	Enables a Cisco IOS voice gateway to authenticate and pass SIP credentials based on the redirecting number when available instead of the calling number of a forwarded call.

voice-class sip bind

To bind the source address of a specific interface for a dial-peer on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip bind** command in dial peer voice configuration mode. To disable bind at the dial-peer level or restore the bind to the global level, use the **no** form of this command.

voice-class sip bind {**control | media**} **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]

no voice-class sip bind {**control | media**}

Syntax Description

control	Binds Session Initiation Protocol (SIP) signaling packets.
media	Binds only media packets.
source-interface *interface-id*	Specifies an interface as the source address of SIP packets.
ipv6-address *ipv6-address*	(Optional) Configures the IPv6 address of the interface.

Command Default

Bind is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **voice-class sip bind** command in dial peer voice configuration mode to bind the source address for signaling and media packets to the IP address of an interface on Cisco IOS voice gateway.

You can configure multiple IPv6 addresses for an interface and select one address using the ipv6-address keyword.

Examples

The following example shows how to configure SIP bind command:

```
Router(config)# dial-peer voice 101 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0
ipv6-address 2001:0DB8:0:1::1
Router(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/0
```

voice-class sip block

To configure an individual dial peer on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE) to drop (not pass) specific incoming Session Initiation Protocol (SIP) provisional response messages, use the **voice-class sip block** command in dial peer voice configuration mode. To disable a configuration to drop incoming SIP provisional response messages on an individual dial peer, use the **no** form of this command.

voice-class sip block {**180** | **181** | **183**} [**sdp** {**absent** | **present**} | **system**]

no voice-class sip block {**180** | **181** | **183**}

Syntax Description

180	Specifies that incoming SIP 180 Ringing messages should be dropped (not passed to the other leg).
181	Specifies that incoming SIP 181 Call is Being Forwarded messages should be dropped (not passed to the other leg).
183	Specifies that incoming SIP 183 Session in Progress messages should be dropped (not passed to the other leg).
sdp	(Optional) Specifies that either the presence or absence of Session Description Protocol (SDP) information in the received response determines when the dropping of specified incoming SIP messages takes place.
absent	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is absent from the received provisional response.
present	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is present in the received provisional response.
system	Configures the dial peer to use global configuration settings for dropping incoming SIP provisional response messages.

Command Default

Defaults to the global configuration setting, which, when not specifically configured, means incoming SIP 180, 181, and 183 provisional responses are forwarded.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced. Only SIP 180 and SIP 183 messages are supported on Cisco UBEs.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. Support was added for SIP 181 messages on the Cisco IOS SIP gateway, SIP-SIP Cisco UBEs, and the SIP trunk of Cisco Unified Communications Manager Express (Cisco Unified CME).
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip block** command in dial peer voice configuration mode to configure a specific dial peer on a Cisco IOS voice gateway or Cisco UBE to override global settings and drop specified SIP provisional response messages. Additionally, you can use the **sdp** keyword to further control when the specified SIP message is dropped based on either the absence or presence of SDP information.

You can also use the **system** keyword to configure a specific dial peer to use global configuration settings for dropping incoming SIP provisional response messages. To configure global settings on a Cisco IOS voice gateway or Cisco UBE, use the **block** command in voice service SIP configuration mode. To disable configurations for dropping specified incoming SIP messages on an individual dial peer, use the **no voice-class sip block** command in dial peer voice configuration mode.

Note This command is supported only on outbound dial peers—it is nonoperational if configured on inbound dial peers. You should configure this command on the outbound SIP leg that sends out the initial INVITE message. Additionally, this feature applies only to SIP-to-SIP calls and will have no effect on H.323-to-SIP calls.

Examples

The following example shows how to configure dial peer 1 to override any global configurations and drop specified incoming SIP provisional response messages regardless whether SDP is present:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 181
```

The following example shows how to configure dial peer 1 to override any global configurations and drop specified incoming SIP provisional response messages only if SDP is present:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 183 sdp present
```

The following example shows how to configure dial peer 1 to override any global configurations and drop incoming SIP provisional response messages only when SDP is not present:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 180 sdp absent
```

The following example shows how to configure a dial peer to use the global configuration settings for dropping incoming SIP provisional response messages:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 181 system
```

The following example shows how to configure a dial peer to pass all incoming SIP provisional response messages regardless of global configuration settings:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# no voice-class sip block 180
```

Related Commands

Command	Description
block	Configures global configuration for dropping specified SIP provisional response messages on a Cisco IOS voice gateway or Cisco UBE.
map resp-code	Configures global settings on a Cisco UBE for mapping specific incoming SIP provisional response messages to a different SIP response message.
voice-class sip map resp-code	Configures a specific dial peer on a Cisco UBE to map specific incoming SIP provisional response messages to a different SIP response message.

voice-class sip call-route

To enable call routing based on the p-called-party-id and history-info header values, at the dial-peer configuration level, use the **voice-class sip call-route** command in dial peer voice configuration mode. To disable header-based routing, use the **no** form of this command.

voice-class sip call-route {**p-called-party-id | history-info**} [**system**]

no voice-class sip call-route {**p-called-party-id | history-info**}

Syntax Description

p-called-party-id	Enables call routing based on the p-called-party-id header.
history-info	Enables call routing based on the history-info header.
system	(Optional) Uses the global configuration settings to enable call routing based on the header values on this dial peer.

Command Default

Support for call routing based on the p-called-party-id and history-info headers at the dial peer level is disabled.

Command Modes

Dial-peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **history-info** keyword was introduced.

Usage Guidelines

Use the **voice-class sip call-route** command on the inbound dial peer, to enable the gateway to route calls based on the received header in a received INVITE message.

The **voice-class sip call-route** command takes precedence over the **call-route** command in voice service VoIP SIP configuration mode. However, if the **voice-class sip call-route** command is used with the **system** keyword, the gateway uses the settings configured globally by the **call-route** command.

Examples

The following example shows how to enable call routing based on the p-called-party-id and history-info header values, at the dial-peer configuration level:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip call-route p-called-party-id
Router(config-dial-peer)# voice-class sip call-route history-info
```

Related Commands

Command	Description
call-route	Enables call routing based on the p-called-party-id and history-info header values at the global configuration level.

voice-class sip calltype-video

To configure the bearer capability setting on an H.320 dial peer so that it supports unrestricted digital media, use the **voice-class sip calltype-video** command in dial peer voice configuration mode. To return the bearer capability setting for an H.320 dial peer to the default, use the **no** form of this command.

voice-class sip calltype-video

no voice-class sip calltype-video

Syntax Description

This command has no arguments or keywords.

Command Default

Bearer capability setting for support of unrestricted digital media support is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

H.320 dial peers support only voice calls by default. Use the **voice-class sip calltype-video** command to configure the bearer capability setting, which enables support of unrestricted digital media calls on an H.320 dial peer.

Examples

The following example shows how to configure the bearer capability setting on dial peer 2 so that it supports unrestricted digital media:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip call-type video
```

voice-class sip copy-list

To configure a list of entities to be sent to the peer call leg on a dial peer, use the **voice-class sip copy-list** command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip copy-list {*tag* | **system**}

no voice-class sip copy-list

Syntax Description

tag	Tag number of the Session Initiation Protocol (SIP) copy list. The range is from 1 to 10000.
system	Specifies to use the global level configuration to copy the list.

Command Default Entries configured at the global level are sent to the peer call leg.

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines Use the **voice-class sip copy-list** command to configure Cisco Unified Border Element (UBE) to pass an unsupported parameter present in a mandatory header from one peer call leg to another. You can copy the inbound message headers into variables and pass the headers to the outbound peer call leg.

Examples The following example shows how to configure a SIP list to be sent to the peer call leg:

```
Router(config)# dial-peer voice 66 voip
Router(config-dial-peer)# voice-class sip copy-list 4
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.

voice-class sip e911

To enable SIP E911 system services on a dial peer, use the **voice-class sip e911** command in VoIP dialpeer configuration mode. To disable SIP E911 services, use the **no** form of this command.

voice-class sip e911

no voice-class sip e911

Syntax Description

This command has no arguments or keywords.

Command Default

The dial peer uses the global setting.

Command Modes

VoIP dialpeer configuration mode.

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **no** form of this command sets the dial peer configuration to disable, which indicates that E911 will not be used for this peer. Because the **no** version of the command causes non default behavior, it can been seen in the **show running-config** output. See also the **voice service voip sip e911** and **debug csm neat** commands.

Examples

The following examples enable and disable E911 services on a VoIP dial peer:

```
Router(config)# dial-peer voice 2
Router(config-dial-peer)# voice-class sip e911

*Jun 06 00:47:20.611: setting peer 2 to enable

Router(config-dial-peer)# no voice-class sip e911

*Jun 06 00:49:58.931: setting peer 2 to disable
```

Related Commands

Command	Description
debug csm neat	Turns on debugging for all Call Switching Module (CSM) Voice over IP (VoIP) calls.
show running-config	Displays the running configuration.
e911	Enables E911 system services for SIP voice service VoIP.

voice-class sip encap clear-channel

To enable RFC 4040-based clear-channel codec negotiation for Session Initiation Protocol (SIP) calls on an individual dial peer, overriding the global setting on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE), use the **voice-class sip encap clear-channel** command in dial peer voice configuration mode. To disable RFC 4040-based clear-channel codec negotiation on an individual dial peer for SIP calls on a Cisco IOS voice gateway or Cisco UBE, use the **no** form of this command.

voice-class sip encap clear-channel [**standard** | **system**]

no voice-class sip encap clear-channel standard

Syntax Description

standard	(Optional) Specifies standard RFC 4040 encapsulation.
system	(Optional) Configures the dial peer to use global configuration settings for clear-channel codec negotiation.

Command Default

The dial peer uses the system configuration. (If the global **encap clear-channel standard** command is not enabled, then legacy encapsulation [X-CCD/8000] is used for clear-channel codec negotiation.)

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip encap clear-channel standard** command in dial peer voice configuration mode to override global settings for clear-channel codec negotiation on a Cisco IOS voice gateway or Cisco UBE and enable RFC 4040-based clear-channel codec negotiation [CLEARMODE/8000] for SIP calls on a specific dial peer. RFC 4040-based clear-channel codec negotiation allows dial peers on Cisco IOS voice gateways and Cisco UBEs to successfully interoperate with third-party SIP gateways that do not support legacy Cisco IOS clear-channel codec encapsulation [X-CCD/8000].

When the **voice-class sip encap clear-channel standard** command is enabled on a specific dial peer on a Cisco IOS voice gateway or Cisco UBE, SIP calls on that dial peer that use the Cisco IOS clear channel codec are translated into calls that use [CLEARMODE/8000] regardless of the global configuration so that the calls do not get rejected when they reach third-party SIP gateways.

You can also use the **voice-class sip encap clear-channel system** command to configure a specific dial peer to use global configuration settings for clear-channel codec negotiation. To enable RFC 4040 clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE, use the **encap clear-channel standard** command in voice service SIP configuration mode. To override global settings and disable RFC 4040-based clear-channel codec negotiation on a specific dial peer, use the **no voice-class sip encap clear-channel standard** command in dial peer voice configuration mode.

Examples

The following example shows how to configure dial peer 1 to override any global configurations and enable RFC 4040-based clear-channel codec negotiation for SIP calls:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip encap clear-channel standard
```

The following example shows how to configure dial peer 1 to use the global configuration for clear-channel codec negotiation for SIP calls:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip encap clear-channel system
```

Related Commands

Command	Description
encap clear-channel standard	Enables RFC 4040-based clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE.

voice-class sip error-code-override

To configure the Session Initiation Protocol (SIP) error code that a dial peer uses for options-keepalive failures or call spike failures, use the **voice-class sip error-code-override** command in dial peer voice configuration mode. To disable the SIP error code configuration, use the **no** form of this command.

voice-class sip error-code-override {**options-keepalive failure | call spike failure**} {*sip-status-code-number* | **system**}

no voice-class sip error-code-override {**options-keepalive failure | call spike failure**}

Syntax Description

options-keepalive failure	(Optional) Configures the SIP error code for options-keepalive failures.
call spike failure	(Optional) Configures the SIP error code for call spike failures.
sip-status-code-number	The SIP status code that is sent for the options keepalive or call spike failure. The range is from 400 to 699. The default value is 503. Table 249 in the "Usage Guidelines" section describes these error codes.
system	Specifies the system configuration used for options-keepalive or call spike failure.

Defaults

By default the SIP error code is not configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The **call spike failure** keyword was added.

Usage Guidelines

The **voice-class sip error-code-override** command in dial peer voice configuration mode configures the error code response for options-keepalive failures and call spike failures at dial peer level. The **error-code-override** command in voice service SIP configuration mode configures the error code responses options-keepalive failures and call spike failures gloablly.

Table 249 describes the SIP error codes.

Table 249 SIP Error Codes

Error Code Number	Description
400	Bad Request
401	Unauthorized
402	Payment Required

Table 249 SIP Error Codes (continued)

Error Code Number	Description
403	Forbidden
404	Not Found
408	Request Timed Out
416	Unsupported URI
480	Temporarily Unavailable
482	Loop Detected
484	Address Incomplete
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
500–599	SIP 5xx—Server/Service Failure
500	Internal Server Error
502	Bad Gateway
503	Service Unavailable
600–699	SIP 6xx—Global Failure

Examples

The following example shows how to configure the SIP error code for options-keepalive failures using the **voice-class sip error-code-override** command:

```
Router(config)# dial-peer voice 432 voip system
Router(config-dial-peer)# voice-class sip error-code-override options-keepalive failure
502
```

The following example shows how to configure the SIP error code for call spike failures using the **voice-class sip error-code-override** command:

```
Router(config)# dial-peer voice 432 voip system
Router(config-dial-peer)# voice-class sip error-code-override call spike failure 502
```

Related Commands

Command	Description
error-code-override	Configures the SIP error code for options-keepalive and call spike failures in voice service SIP and dial peer voice configuration mode, respectively.

voice-class sip g729 annexb-all

To configure settings on a Cisco IOS Session Initiation Protocol (SIP) gateway that determine if a specific dial peer on the gateway treats the G.729br8 codec as superset of G.729r8 and G.729br8 codecs for interoperation with Cisco Unified Communications Manager, use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode. To prevent a dial peer from treating the G.729br8 codec as a superset of the G.729r8 and G.729br8 codecs, use the **no** form of this command.

voice-class sip g729 annexb-all [**system**]

no voice-class sip g729 annexb-all

Syntax Description

annexb-all	Specifies that the G.729br8 codec is treated as a superset of G.729r8 and G.729br8 codecs to communicate with Cisco Unified Communications Manager.
system (default)	(Optional) Specifies that the dial peer allow communication between incompatible G.729 codecs according to global settings configured for this feature on the Cisco IOS SIP gateway.

Command Default

The dial peer defers to global (system) settings for the Cisco IOS gateway.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

There are four variations of the G.729 coder-decoder (codec), which fall into two categories:

High Complexity

- G.729 (g729r8)—a high complexity algorithm codec on which all other G.729 codec variations are based.
- G.729 Annex-B (g729br8 or G.729B)—a variation of the G.729 codec that allows the DSP to detect and measure voice activity and convey suppressed noise levels for re-creation at the other end. Additionally, the Annex-B codec includes Internet Engineering Task Force (IETF) voice activity detection (VAD) and comfort noise generation (CNG) functionality.

Medium Complexity

- G.729 Annex-A (g729ar8 or G.729A)—a variation of the G.729 codec that sacrifices some voice quality to lessen the load on the DSP. All platforms that support G.729 also support G.729A.
- G.729A Annex-B (g729abr8 or G.729AB)—a variation of the G.729 Annex-B codec that, like G.729B, sacrifices voice quality to lessen the load on the DSP. Additionally, the G.729AB codec also includes IETF VAD and CNG functionality.

The VAD and CNG functionality is what causes the instability during communication attempts between two DSPs where one DSP is configured with Annex-B (G.729B or G.729AB) and the other without (G.729 or G.729A). All other combinations interoperate. To configure a dial peer on a Cisco IOS SIP gateway for interoperation with Cisco Unified Communications Manager (formerly known as the Cisco CallManager, or CCM), use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode to do one of the following:

- Override global settings for a Cisco IOS gateway and configure the dial peer to accept and connect calls between two DSPs with incompatible G.729 codecs.
- Specify that an individual dial peer use the global (**system**) settings on the Cisco IOS SIP gateway.
- Use the no form of the command to override global settings for the Cisco IOS gateway and specify that the dial peer does not treat the G.729br8 codec as a superset of G.729r8 and G.729br8 codecs.

Use the **g729 annexb-all** command in voice service SIP configuration mode to configure the global settings for the Cisco IOS SIP gateway.

Examples

The following example shows how to configure a dial peer on a Cisco IOS SIP gateway to connect calls between two DSPs using incompatible G.729 codecs, overriding global gateway settings for this feature:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1
Router(config-dial-peer)# voice-class sip g729 annexb-all
```

Related Commands

Command	Description
g729 annexb-all	Configure global settings that determine if a Cisco IOS SIP gateway treats the G.729br8 codec as superset of G.729r8 and G.729br8 codecs.

voice-class sip history-info

To enable Session Initiation Protocol (SIP) history-info header support on the Cisco IOS gateway at the dial-peer level, use the **voice-class sip history-info** command in dial peer configuration mode. To disable SIP history-info header support, use the **no** form of this command.

voice-class sip history-info [**system**]

no voice-class sip history-info

Syntax Description

system	(Optional) Enables history-info support using global configuration settings.

Command Default

History-info header support is disabled.

Command Modes

Dial peer configuration (conf-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use this command to enable history-info header support at the dial-peer level. The history-info header (as defined in RFC 4244) records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.

Note The Cisco IOS SIP gateway cannot use the information in the history-info header to make routing decisions.

Examples

The following example enables SIP history-info header support at the dial-peer level:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip history-info
```

The following example enables SIP history-info header support at the dial-peer level using the global configuration settings:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip history-info system
```

Related Commands

Command	Description
history-info	Enables SIP history-info header support on Cisco IOS gateway at a global level.

voice-class sip localhost

To configure individual dial peers to override global settings on Cisco IOS voice gateways, Cisco Unified Border Elements (Cisco UBEs), or Cisco Unified Communications Manager Express (Cisco Unified CME) and substitute a Domain Name System (DNS) hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **voice-class sip localhost** command in dial peer voice configuration mode. To disable substitution of a localhost name on a specific dial peer, use the **no** form of this command. To configure a specific dial peer to defer to global settings for localhost name substitution, use the **default** form of this command.

voice-class sip localhost dns:[*hostname.*]*domain* [**preferred**]

no voice-class sip localhost

default voice-class sip localhost

Syntax Description

dns:[*hostname.*]*domain*	Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages. This value can be the hostname and the domain separated by a period (**dns:***hostname.domain*) or just the domain name (**dns:***domain*). In both case, the **dns:** delimiter must be included as the first four characters.
preferred	(Optional) Designates the specified DNS hostname as preferred.

Command Default

The dial peer uses the global configuration setting to determine whether a DNS localhost name is substituted in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)XA	This command was modified. The **preferred** keyword was added to specify the preferred localhost if multiple registrars are configured on a SIP trunk.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip localhost** command in dial peer voice configuration mode to override the global configuration on Cisco IOS voice gateways, Cisco UBEs, or Cisco Unified CME and configure a DNS localhost name to be used in place of the physical IP address in the From, Call-ID, and Remote-Party-ID

headers of outgoing messages on a specific dial peer. When multiple registrars are configured for an individual dial peer you can then use the **voice-class sip localhost preferred** command to specify which host is preferred for that dial peer.

To globally configure a localhost name on a Cisco IOS voice gateway, Cisco UBE, or Cisco Unified CME, use the **localhost** command in voice service SIP configuration mode. Use the **no voice-class sip localhost** command to remove localhost name configurations for the dial peer and to force the dial peer to use the physical IP address in the host portion of the From, Call-ID, and Remote-Party-ID headers regardless of the global configuration.

Examples

The following example shows how to configure dial peer 1 (overriding any global configuration) to substitute a domain (no hostname specified) as the preferred localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip localhost dns:example.com preferred
```

The following example shows how to configure dial peer 1 (overriding any global configuration) to substitute a specific hostname on a domain as the preferred localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip localhost dns:MyHost.example.com preferred
```

The following example shows how to force dial peer 1 (overriding any global configuration) to use the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# no voice-class sip localhost
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.

voice-class sip map resp-code

To configure an individual dial peer on a Cisco Unified Border Element (Cisco UBE) to map specific received Session Initiation Protocol (SIP) provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer, use the **voice-class sip map resp-code** command in dial peer voice configuration mode. To disable mapping of received SIP provisional response messages on an individual dial peer, use the **no** form of this command. To configure a specific dial peer to defer to global settings for mapping of incoming SIP provisional response messages, use the **default** form of this command.

voice-class sip map resp-code 181 to 183

no voice-class sip map resp-code 181 to 183

default voice-class sip map resp-code 181 to 183

Syntax Description

181	The code representing the specific incoming SIP provisional response messages to be mapped and replaced.
to	The designator for specifying that the specified incoming SIP provisional response message should be mapped to and replaced with a different SIP provisional response message on the outgoing SIP dial peer.
183	The code representing the specific SIP provisional response message on the outgoing dial peer to which incoming SIP message responses should be mapped.

Command Default

Mapping behavior is determined by the global configuration setting, which, if not specifically configured, means that incoming SIP provisional responses are passed, as is to the outbound SIP dial peer.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip map resp-code** command in dial peer voice configuration mode to configure an individual dial peer on a Cisco UBE to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outgoing SIP dial peer.

Note If the **block** command is configured for incoming SIP 181 messages, either globally or at the dial-peer level, the messages may be dropped before they can be passed or mapped to a different message—even when the **voice-class sip map resp-code** command is enabled. To globally configure whether and when incoming SIP 181 messages are dropped, use the **block** command in voice service SIP configuration mode (or use the **voice-class sip block** command in dial peer voice configuration mode to configure drop settings on individual dial peers).

To configure mapping of SIP provisional response messages globally on a Cisco UBE, use the **map resp-code** command in voice service SIP configuration mode. To disable mapping of SIP 181 message for an individual dial peer on a Cisco UBE, use the **no voice-class sip map resp-code** command in voice service SIP configuration mode.

As an example, to enable interworking of SIP endpoints that do not support the handling of SIP 181 provisional response messages, you could use the **block** command to configure a Cisco UBE to drop SIP 181 provisional response messages received on the SIP trunk or you can use the **map resp-code** command to configure the Cisco UBE to map the incoming messages to and send out, instead, SIP 183 provisional response messages to the SIP line in Cisco Unified Communications Manager Express (Cisco Unified CME).

Note This command is supported only for SIP-to-SIP calls and will have no effect on H.323-to-SIP or time-division multiplexing (TDM)-to-SIP calls.

Examples

The following example shows how to configure dial peer 1 to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outbound dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip map resp-code 181 to 183
```

Related Commands

Command	Description
block	Configures global settings for dropping specific SIP provisional response messages on a Cisco IOS voice gateway or Cisco UBE.
map resp-code	Configures global settings on a Cisco UBE for mapping specific incoming SIP provisional response messages to a different SIP response message.
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or Cisco UBE to drop specified SIP provisional response messages.

voice-class sip options-keepalive

To monitor connectivity between Cisco Unified Border Element VoIP dial-peers and SIP servers to, use the **voice-class sip options-keepalive** command in dial peer configuration mode. To disable monitoring connectivity, use the **no** form of this command.

voice-class sip options-keepalive [**up-interval** *seconds* | **down-interval** *seconds*] [**retry** *retries*]

no voice-class sip options-keepalive

Syntax Description

up-interval *seconds*	Number of up-interval seconds allowed to pass before marking the UA as unavailable.This keyword is effective when the dial-peer is up (not busied out). The range is 5-1200. The default is 60.
down-interval *seconds*	Number of down-interval seconds allowed to pass before marking the UA as available. This keyword is effective when the dial-peer is down (busied out). The range is 5-1200. The default is 30.
retry *retries*	Number of retry attempts before changing the state of UA. The range is 1 to 10. The default is 5 attempts.

Command Default

The dial-peer is active (UP).

Command Modes

Dial peer configuration mode (config-dial-peer).

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **voice-class sip options-keepalive** command to configure a out-of-dialog (OOD) Options Ping mechanism between any number of destinations. When monitored endpoint heartbeat responses fails, the configured dial-peer is busied out. If there is a alternate dial-peer configured for the same destination pattern, the call is failed over to the next preference dial peer or the on call is rejected with an error cause code.

The response to options ping will be considered unsuccessful and dial-peer will be busied out for following scenarios:

Table 250 Error Codes that busyout the endpoint

Error Code	Description
503	service unavailable
505	sip version not supported
no response	i.e. request timeout

All other error codes, including 400 are considered a valid response and the dial peer is not busied out.

Examples

The following example shows a sample configuration of dial peer 100 configured to reset:

```
dial-peer voice 100 voip
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer and specifies the method of voice encapsulation

voice-class sip outbound-proxy

To configure an outbound proxy, use the **voice-class sip outbound-proxy** command in dial peer configuration mode. To reset the outbound proxy value to its default, use the **no** form of this command.

voice-class sip outbound-proxy {**dhcp** | **ipv4:***ipv4-address* | **ipv6:[***ipv6-address***]** | **dns:***host***:***domain*} [**:***port-number*]

no voice-class sip outbound-proxy

Syntax Description

dhcp	Specifies that the outbound-proxy IP address is retrieved from a DHCP server.
ipv4:*ipv4-address*	Configures proxy on the server, sending all initiating requests to the specified IPv4 address destination. The colon is required.
ipv6:[*ipv6-address***]**	Configures proxy on the server, sending all initiating requests to the specified IPv6 address destination. Brackets must be entered around the IPv6 address. The colon is required.
dns:*host***:***domain*	Configures proxy on the server, sending all initiating requests to the specified domain destination. The colons are required.
:*port-number*	(Optional) Port number for the Session Initiation Protocol (SIP) server. The colon is required.

Command Default

An outbound proxy is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip outbound-proxy** command, in dial peer configuration mode, takes precedence over the command in SIP global configuration mode.

Brackets must be entered around the IPv6 address.

Examples

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an IPv4 address (10.1.1.1) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy ipv4:10.1.1.1
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate a domain (sipproxy:cisco.com) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dns:sipproxy:cisco.com
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an outbound proxy using DHCP:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
voice service	Enters voice-service configuration mode and specifies a voice encapsulation type.

voice-class sip preloaded-route

To enable preloaded route support for dial-peer Session Initiation Protocol (SIP) calls, use the **voice-class sip preloaded-route** command in dial peer voice configuration mode. To reset to the default value, use the **no** form of this command.

voice-class sip preloaded-route {[**sip-server**] **service-route** | **system**}

no voice-class sip preloaded-route

Syntax Description

sip-server	(Optional) Adds SIP server information to the Route header.
service-route	Adds the Service-Route information to the Route header.
system	Uses the global system value. This is the default.

Command Default

SIP calls at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip preloaded-route** command takes precedence over the **preloaded-route** command configured in SIP configuration mode. However, if the **voice-class sip preloaded-route** command is used with the **system** keyword, the gateway uses the global settings configured by the **preloaded-route** command.

Examples

The following example shows how to configure the dial peer to include SIP server and Service-Route information in the Route header:

```
dial-peer voice 102 voip
 voice-class sip preloaded-route sip-server service-route
```

The following example shows how to configure the dial peer to include only Service-Route information in the Route header:

```
dial-peer voice 102 voip
 voice-class sip preloaded-route service-route
```

Related Commands

Command	Description
preloaded-route	Enables preloaded route support for VoIP SIP calls.

voice-class sip privacy

To set privacy support at the dial-peer level as defined in RFC 3323, use the **voice-class sip privacy** command in dial peer configuration mode. To remove privacy support as defined in RFC 3323, use the **no** form of this command.

voice-class sip privacy {**disable** | **pstn** | **system** | *privacy-option* [**critical**]}

no voice-class sip privacy

Syntax Description

disable	Disables the privacy service for this dial peer regardless of prior implementations. When selected, this becomes the only valid option.
pstn	Requests that the privacy service implements a privacy header using the default Public Switched Telephone Network (PSTN) rules for privacy (based on information in Octet 3a). When selected, this becomes the only valid option.
system	Uses the global configuration settings to enable the privacy service on this dial peer. When selected, this becomes the only valid option.
privacy-option	The privacy support options to be set at the dial-peer level. The following keywords can be specified for the *privacy-option* argument: • **header** — Requests that privacy be enforced for all headers in the Session Initiation Protocol (SIP) message that might identify information about the subscriber. • **history** — Requests that the information held in the history-info header is hidden outside the trust domain. • **id** — Requests that the Network Asserted Identity that authenticated the user be kept private with respect to SIP entities outside the trusted domain. • **session** — Requests that the information held in the session description is hidden outside the trust domain. • **user** — Requests that privacy services provide a user-level privacy function. **Note** The keywords can be used alone, altogether, or in any combination with each other, but each keyword can be used only once.
critical	(Optional) Requests that the privacy service performs the specified service or fail the request. **Note** This optional keyword is only available after at least one of the *privacy-option* keywords (**header**, **history**, **id**, **session**, or **user**) has been specified and can be used only once per command.

Command Default Privacy support is disabled.

Command Modes Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	The **history** keyword was added to provide support for the history-info header information.

Usage Guidelines

Use the **voice-class sip privacy** command to instruct the gateway to add a Proxy-Require header, set to a value supported by RFC 3323, in outgoing SIP request messages at the dial-peer level.

Use the **voice-class sip privacy critical** command to instruct the gateway to add a Proxy-Require header with the value set to critical. If a user agent sends a request to an intermediary that does not support privacy extensions, the request fails.

The **voice-class sip privacy** command takes precedence over the **privacy** command in voice service voip sip configuration mode. However, if the **voice-class sip privacy** command is used with the **system** keyword, the gateway uses the settings configured globally by the **privacy** command.

Examples

The following example shows how to disable the privacy on dial peer 2:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip privacy disable
```

The following example shows how to configure the **voice-class sip privacy** command so that the information held in the history-info header is hidden outside the trust domain:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip privacy history
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAI or PPI privacy headers in outgoing SIP requests or response messages.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.
clid (voice-service-voip)	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, removes the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allows a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers.
privacy	Sets privacy support at the global level as defined in RFC 3323.

voice-class sip privacy-policy

To configure the privacy header policy options at the dial-peer level, use the **voice-class sip privacy-policy** command in dial peer voice configuration mode. To disable privacy-policy options, use the **no** form of this command.

voice-class sip privacy-policy {**passthru | send-always | strip {diversion | history-info}**} [**system**]

no voice-class sip privacy-policy {**passthru | send-always | strip {diversion | history-info**}}

Syntax Description

passthru	Passes the privacy values from the received message to the next call leg.
send-always	Passes a privacy header with a value of None to the next call leg, if the received message does not contain privacy values but a privacy header is required.
strip	Strip the diversion or history-info headers received from the next call leg.
diversion	Strip the diversion header received from the next call leg.
history-info	Strip the history-info header received from the next call leg.
system	(Optional) Uses the global configuration settings to configure the dial peer.

Command Default

No privacy-policy settings are configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T. The **strip**, **diversion**, and **history-info** keywords were added.

Usage Guidelines

If a received message contains privacy values, use the **voice-class sip privacy-policy passthru** command to ensure that the privacy values are passed from one call leg to the next. If a received message does not contain privacy values but the privacy header is required, use the **voice-class sip privacy-policy send-always** command to set the privacy header to None and forward the message to the next call leg. You can configure the system to support both options at the same time.

The **voice-class sip privacy-policy** command takes precedence over the **privacy-policy** command in voice service voip sip configuration mode. However, if the **voice-class sip privacy-policy** command is used with the **system** keyword, the gateway uses the settings configured globally by the **privacy-policy** command.

Examples

The following example shows how to enable the pass-through privacy policy on the dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
```

The following example shows how to enable the pass-through, send-always, and strip policies on the dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
Router(config-dial-peer)# voice-class sip privacy-policy send-always
Router(config-dial-peer)# voice-class sip privacy-policy strip diversion
Router(config-dial-peer)# voice-class sip privacy-policy strip history-info
```

The following example shows how to enable the send-always privacy policy on the dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy send-always
```

The following example shows how to enable both the pass-through privacy policy and send-always privacy policies on the dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
Router(config-dial-peer)# voice-class sip privacy-policy send-always
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAID or PPID privacy headers in outgoing SIP requests or response messages.
privacy-policy	Configures the privacy header policy options at the global configuration level.

voice-class sip random-contact

To populate the outgoing INVITE message with random-contact information (instead of clear contact information) at the dial-peer level, use the **voice-class sip random-contact** command in dial peer voice configuration mode. To disable random contact information, use the **no** form of this command.

voice-class sip random-contact [**system**]

no voice-class sip random-contact

Syntax Description

system	(Optional) Uses the global configuration settings to populate the INVITE message with random contact information.

Command Default

Support for random contact at the dial-peer level uses the the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

To populate outbound INVITE messages (from the Cisco Unified Border Element) with random-contact information instead of clear-contact information at the dial-peer level, use the **voice-class sip random-contact** command. This functionality will work only when the Cisco Unified Border Element is configured for SIP registration with random-contact, using the **credentials** and **registrar** commands.

The **voice-class sip random-contact** command takes precedence over the **random-contact** command in voice service voip sip configuration mode. However, if the **voice-class sip random-contact** command is used with the **system** keyword, the gateway uses the settings configured globally by the **random-contact** command.

Examples

The following example shows how to populate outbound INVITE messages, at the dial-peer level, with random-contact information:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip random-contact
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
random-contact	Populates the outgoing INVITE message with random contact information at the global level.

voice-class sip random-request-uri validate

To enable the validation of the called-number based on the random value generated during the registration of the number, at dial-peer configuration level, use the **voice-class sip random-request-uri validate** command in dial peer voice configuration mode. To disable validation, use the **no** form of this command.

voice-class sip random-request-uri validate [**system**]

no voice-class sip random-request-uri validate

Syntax Description

system	(Optional) Uses the global configuration settings to enable called-number validation on this dial peer.

Command Default

Validation is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The system generates a random string when registering a new number. An INVITE message with the P-Called-Party-ID value can have the Request-URI set to this random number. To enable the system to identify the called number from the random number in the Request-URI, use the **voice-class sip random-request-uri validate** command on the inbound dial peer.

If the P-Called-Party-ID is not set in the INVITE message, the Request URI for that message must contain the called party information (and cannot contain a random number). Therefore validation is performed only on INVITE messages with a P-Called-Party-ID.

The **voice-class sip random-request-uri validate** command takes precedence over the **random-request-uri validate** command in voice service voip sip configuration mode. However, if the **voice-class sip random-request-uri validate** command is used with the **system** keyword, the gateway uses the settings configured globally by the **random-request-uri validate** command.

Examples

The following example shows how to enable call routing based on the P-Called-Party-ID header value at the dial-peer configuration level:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip random-request-uri validate
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
random-request-uri validate	Validates the called number based on the random value generated during the registration of the number at the global configuration level.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.

voice-class sip registration passthrough

To configure Session Initiation Protocol (SIP) registration pass-through options on a dial peer, use the **voice-class sip registration passthrough** command in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip registration passthrough [[**static**] [**rate-limit** [**expires** *value*] [**fail-count** *value*]] [**registrar-index** [*index*]] | **system**]

no voice-class sip registration passthrough

Syntax Description

static	(Optional) Configures Cisco Unified Border Element (UBE) to use static registrar details for SIP registration. Cisco UBE works in point-to-point mode when the **static** keyword is used.
rate-limit	(Optional) Configures SIP registration pass-through rate-limiting options.
expires *value*	(Optional) Sets the expiry value for rate limiting, in seconds. The range is from 60 to 65535. The default is 3600.
fail-count *value*	(Optional) Sets the fail-count value for rate limiting. The range is from 2 to 20. The default is 0.
registrar-index	(Optional) Configures the registrar index used for registration pass-through.
index	(Optional) Registration index value. The range is from 1 to 6.
system	(Optional) Uses global registration pass-through configuration to configure the SIP registration pass-through options.

Command Default

SIP registration pass-through options that are configured at the global level are configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

You can use the **voice-class sip registration passthrough** command to configure the following SIP pass-through functionalities on a dial peer:

- Back-to-back registration facility to register phones for call routing.
- Options to configure the rate-limiting values, such as the expiry time, fail-count, and a list of registrars to be used for registration.

Examples

The following example shows how to set the registrar index of 1 for the SIP registration pass-through rate limiting:

```
Router# configure terminal
Router(config)# dial-peer voice 444 voip
Router(config-dial-peer)# voice-class sip registration passthrough static rate-limit
registrar-index 1
```

Related Commands

Command	Description
registration passthrough	Configures SIP registration pass-through options at the global level.

voice-class sip rel1xx

To enable all Session Initiation Protocol (SIP) provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint, use the **voice-class sip rel1xx** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

voice-class sip rel1xx {**supported** *value* | **require** *value* | **system** | **disable**}

no sip rel1xx

Syntax Description

supported *value*	Supports reliable provisional responses. The *value* argument may have any value, as long as both the user-agent client (UAC) and user-agent server (UAS) configure it the same.
require *value*	Requires reliable provisional responses. The *value* argument may have any value, as long as both the UAC and UAS configure it the same.
system	Uses the value configured in voice service mode. This is the default.
disable	Disables the use of reliable provisional responses.

Command Default

system

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

There are two ways to configure reliable provisional responses:

- Dial-peer mode. You can configure reliable provisional responses for the specific dial peer only by using the **voice-class sip rel1xx** command.
- SIP mode. You can configure reliable provisional responses globally by using the **rel1xx** command.

The use of resource reservation with SIP requires that the reliable provisional feature for SIP be enabled either at the VoIP dial-peer level or globally on the router.

This command applies to the dial peer under which it is used or points to the global configuration for reliable provisional responses. If the command is used with the **supported** keyword, the SIP gateway uses the Supported header in outgoing SIP INVITE requests. If it is used with the **require** keyword, the gateway uses the Required header.

This command, in dial peer configuration mode, takes precedence over the **rel1xx** command in global configuration mode with one exception: If this command is used with the **system** keyword, the gateway uses what was configured under the **rel1xx** command in global configuration mode.

Examples

The following example shows how to use this command on either an originating or a terminating SIP gateway:

- On an originating gateway, all outgoing SIP INVITE requests matching this dial peer contain the Supported header where *value* is 100rel.
- On a terminating gateway, all received SIP INVITE requests matching this dial peer support reliable provisional responses.

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip rel1xx supported 100rel
```

Related Commands

Command	Description
rel1xx	Provides provisional responses for calls on all VoIP calls.

voice-class sip reset timer expires

To configure an individual dial peer on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE) to reset the expires timer upon receipt of a Session Initiation Protocol (SIP) 183 Session In Progress message, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode. To globally disable resetting of the expires timer upon receipt of SIP 183 messages, use the **no** form of this command.

voice-class sip reset timer expires 183

no voice-class sip reset timer expires 183

Syntax Description

183	Specifies resetting of the expires timer upon receipt of SIP 183 Session In Progress messages.

Command Default

The expires timer is not reset after receipt of SIP 183 Session In Progress messages and a session or call that is not connected within the default expiration time (three minutes) is dropped.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

In some scenarios, early media cut-through calls (such as emergency calls) rely on SIP 183 with session description protocol (SDP) Session In Progress messages to keep the session or call alive until receiving a FINAL SIP 200 OK message, which indicates that the call is connected. In these scenarios, the call can time out and be dropped if it does not get connected within the default expiration time (three minutes).

Note The expires timer default is three minutes. However, you can configure the expiration time to a maximum of 30 minutes using the **timers expires** command in SIP user agent (UA) configuration mode.

To prevent early media cut-through calls from being dropped on a specific dial peer because they reach the expires timer limit, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode.

To globally configure all dial peers on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE so that the expires timer is reset upon receipt of any SIP 183 message, use the **reset timer expires** command in voice service SIP configuration mode. To disable resetting of the expires timer on receipt of SIP 183 messages for an individual dial peer, use the **no voice-class sip reset timer expires** command in dial peer voice configuration mode.

Examples

The following example shows how to configure dial peer 1 on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer each time a SIP 183 message is received:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip reset timer expires 183
```

Related Commands

Command	Description
reset timer expires	Globally configures Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer upon receipt of a SIP 183 message.
timers expires	Specifies how long a SIP INVITE request remains valid before it times out if no appropriate response is received for keeping the session alive.

voice-class sip resource priority mode (dial peer)

To push the user access server (UAS) to operate in a loose or strict mode, use the **voice-class sip resource priority mode** command in dial peer voice configuration mode. To disable the **voice-class sip resource priority mode**, use the **no** form of this command.

voice-class sip resource priority mode [**loose** | **strict**]

no voice-class sip resource priority mode [**loose** | **strict**]

Syntax Description

loose	(Optional) In the loose mode, unknown values of name space or priority values received in the Resource-Priority header in Session Initiation Protocol (SIP) requests are ignored by the gateway. The request is processed as if the Resource-Priority header was not present.
strict	(Optional) In the strict mode, unknown values of name space or priority values received in the Resource-Priority header in SIP requests are rejected by the gateway using a SIP response code 417 (Unknown Resource-Priority) message response. An Accept-Resource-Priority header enumerating the supported name space and values is included in the 417 message response.

Command Default

The default value is **loose mode**.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

When the **no** version of this command is executed, the call operates in the **loose** mode.

Examples

The following example shows how to set up the **voice-class sip resource priority mode** command in loose mode:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority mode loose
```

The following example shows how to set up the **voice-class sip resource priority mode** command in strict mode:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority mode strict
```

Related Commands

Command	Description
voice-class sip resource priority namespace	Priorities mandatory call prioritization handling for initial original INVITE message requests.

voice-class sip resource priority namespace (dial peer)

To prioritize mandatory call prioritization handling for initial original INVITE message requests, use the **voice-class sip resource priority namespace** command in dial peer voice configuration mode. To disable the **voice-class sip resource priority namespace** command, use the **no** form of this command.

voice-class sip resource priority namespace [**drsn | dsn | q735**]

no voice-class sip resource priority namespace [**drsn | dsn | q735**]

Syntax Description

drsn	(Optional) U. S. Defense Red Switched Network (DRSN).
dsn	(Optional) U. S. Defense Switched Network (DSN).
q735	(Optional) International Telecommunications Union, *Stage 3 description for community of interest supplementary services using Signaling System No. 7: Multilevel precedence and preemption, Recommendation Q.735.3*, March 1993.

Command Default

When the **no** version of this command is executed using namespace, the Cisco IOS gateway transparently passes the multilevel precedence and preemption (MLPP) values that were received on the PSTN side.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

When the **no** version of this command is executed using the namespace, the Cisco IOS gateway transparently passes the multilevel precedence and preemption (MLPP) values that were received on the PSTN side.

Examples

The following example shows how to set up the **voice-class sip resource priority namespace** command in the U. S. DSN format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace dsn
```

The following example shows how to set up the **voice-class sip resource priority namespace** command in the U. S. DRSN format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace drsn
```

The following example shows how to set up the **voice-class sip resource priority namespace** command in the Public SS7 Network format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace q735
```

Related Commands

Command	Description
voice-class sip resource priority mode	Pushes the UAS to operate in a loose or strict mode.

voice-class sip rsvp-fail-policy

To specify the action that takes place at the dial peer level on a Cisco IOS Session Initiation Protocol (SIP) gateway when Resource Reservation Protocol (RSVP) negotiation fails, use the **voice-class sip rsvp-fail-policy** command in dial peer configuration mode. To reset failure behavior to the default settings, use the **no** form of this command.

voice-class sip rsvp-fail-policy {**video** | **voice**} **post-alert** {**optional keep-alive** | **mandatory** {**keep-alive** | **disconnect retry** *retry-attempts*}} **interval** *seconds*

no voice-class sip rsvp-fail-policy {**video** | **voice**} **post-alert** {**optional** [**keep-alive**] | **mandatory** [**keep-alive** | **disconnect retry** *retry-attempts*]} [**interval** *seconds*]

Syntax Description

video	Specifies the video RSVP stream type.
voice	Specifies the audio or fax RSVP stream type.
post-alert	Specifies that behavior takes place only when the call state is post alert.
optional	Specifies that behavior takes place when RSVP fails even if RSVP negotiation is optional.
mandatory	Specifies that behavior takes place when RSVP fails only if RSVP negotiation is mandatory.
keep-alive	Specifies the sending of keepalive messages when RSVP fails.
disconnect	Specifies that the call is disconnected if RSVP fails after the specified number of retry settings.
retry	Specifies the number of reconnection attempts before disconnecting the call.
retry-attempts	The number of retry attempts. Valid entries are from 1 to 100.
interval	Specifies the interval between keepalive or retry attempts.
seconds	The retry interval in seconds. Valid entries are from 5 to 3600.

Command Default

Keepalive messages are sent at 30-second intervals when a post alert voice or video call fails to negotiate RSVP regardless of the RSVP negotiation setting (mandatory or optional).

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use this command to configure call handling behavior when a call fails RSVP negotiation. You can configure the behavior that takes place for either optional or mandatory RSVP negotiation but the behavior will apply only to calls in a post alert call state. To configure the behavior that takes place when RSVP negotiation fails, use the **voice-class sip rsvp-fail-policy** command in dial peer configuration mode.

If a call fails RSVP negotiation where negotiation is optional, then RSVP negotiation should be retried using the keepalive function at specified intervals until RSVP negotiation is successful.

If a call fails RSVP negotiation where negotiation is mandatory, then RSVP negotiation should be configured in one of two ways:

- The call that failed RSVP negotiation is disconnected after a specified number of attempts to renegotiate RSVP with each retry taking place at a specified interval. If negotiation succeeds during these retry attempts, counters and timers are reset to zero.
- The call that failed RSVP negotiation is kept alive with keepalive messages sent at specified intervals until negotiation is successful.

Examples

The following example shows how to specify sending of keepalive messages at 60-second intervals for a call that fails RSVP negotiation when negotiation is optional:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip rsvp-fail-policy voice post-alert optional
keep-alive interval 60
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
handle-replaces	Configures fallback to legacy handling of SIP INVITE.
ip qos defending-priority	Configures the RSVP defending priority value.
ip qos dscp	Sets the DSCP value for QoS.
ip qos policy-locator	Configures application-specific reservations (application IDs) used for specifying bandwidth reservations.
ip qos preemption-priority	Configures the RSVP preemption priority value.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.
show-sip-ua calls	Displays the active UAC and UAS information on SIP calls.

voice-class sip tel-config to-hdr

To configure the To: Header (to hdr) request Uniform Resource Identifier (URI) to telephone (TEL) format for dial-peer VoIP Session Initiation Protocol (SIP) calls, use the **voice-class sip tel-config to-hdr** command in dial peer voice configuration mode. To reset to the default, use the **no** form of this command.

voice-class sip tel-config to-hdr {**phone-context** | **system**}

no voice-class sip tel-config to-hdr

Syntax Description

phone-context	Appends the phone context parameter to the TEL URL on a dial-peer basis.
system	Uses the system value. This is the default.

Command Default

The To: Header request URIs at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip tel-config to-hdr** command takes precedence over the **tel-config to-hdr** command configured in SIP configuration mode. However, if the **voice-class sip tel-config to-hdr** command is used with the **system** keyword, the gateway uses the global settings configured by the **tel-config to-hdr** command.

Examples

The following example configures the To: header in TEL format for a dial peer VoIP SIP call, and appends the phone-context parameter:

```
dial-peer voice 102 voip
 voice-class sip tel-config to-hdr phone-context
```

Related Commands

Command	Description
tel-config to-hdr	Configures the To: Header Request URI to telephone format for VoIP SIP calls.

voice-class sip transport switch

To enable switching between UDP and TCP transport mechanisms for large Session Initiation Protocol (SIP) messages for a specific dial peer, use the **voice-class sip transport switch** command in dial peer configuration mode. To disable switching between UDP and TCP transport mechanisms for large SIP messages for a specific dial peer, use the **no** form of this command.

voice-class sip transport switch udp tcp

no voice-class sip transport switch udp tcp

Syntax Description

udp	Enables switching transport from UDP on the basis of the size of the SIP request being greater than the MTU size.
tcp	Enables switching transport to TCP.

Command Default

Disabled.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **voice-class sip transport switch** command takes precedence over the global **transport switch** command.

Examples

The following example shows how to set up the **voice-class sip transport switch** command:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip transport switch udp tcp
```

Related Commands

Command	Description
debug ccsip transport	Enables tracing of the SIP transport handler and the TCP or UDP process.
transport switch	Enables switching between transport mechanisms globally if the SIP message is larger than 1300 bytes.

voice-class sip url

To configure URLs to either the Session Initiation Protocol (SIP), SIP security (SIPS), or telephone (TEL) format for your dial-peer SIP calls, use the **voice-class sip url** command in dial peer voice configuration mode. To reset to the default value use the **no** form of this command.15.0(1)M

voice-class sip url {**sip** | **sips** | **tel** [**phone-context**] | **system**}

no voice-class sip url

Syntax Description

sip	Generates URLs in the SIP format for calls on a dial-peer basis.
sips	Generates URLs in the SIPS format for calls on a dial-peer basis.
tel	Generates URLs in the TEL format for calls on a dial-peer basis.
phone-context	(Optional) Appends the phone context parameter to the TEL URL on a dial-peer basis.
system	Uses the system value. This is the default.

Command Default

SIP calls at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.4(6)T	The **sips** keyword was added.
12.4(22)YB	The **phone-context** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice-call connections.

The **voice-class sip url** command takes precedence over the **url** command configured in SIP configuration mode. However, if the **voice-class sip url** command is used with the **system** keyword, the gateway uses what was globally configured with the **url** command.

Examples

The following example shows how to configure the **voice-class sip url** command to generate URLs in the SIP format:

```
dial-peer voice 102 voip
 voice-class sip url sip
```

The following example shows how to configure the **voice-class sip url** command to generate URLs in the SIPS format:

```
dial-peer voice 102 voip
 voice-class sip url sips
```

The following example shows how to configure the **voice-class sip url** command to generate URLs in the TEL format:

```
dial-peer voice 102 voip
 voice-class sip url tel
```

The following example shows how to configure the **voice-class sip url** command to generate URLs in the TEL format, and append the phone-context parameter:

```
dial-peer voice 102 voip
 voice-class sip url tel phone-context
```

Related Commands

Command	Description
sip url	Generates URLs in the SIP, SIPS, or TEL format.
url	Configures URLs to either SIP, SIPS, or TEL format.

voice-class source interface

To allow a loopback interface to be associated with a VoIP or VoIPv6 dial-peer profile, use the **voice-class source interface** command in dial peer configuration mode. To disable this association, use the **no** form of this command.

voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

no voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

Syntax Description

loopback	Specifies the loopback interface address.
interface-id	Specifies the interface on which the address is to be configured.
ipv4-address	(Optional) IPv4 address used in the loopback interface address.
ipv6-address	(Optional) IPv6 address used in the loopback interface address.

Command Default

No loopback interface is associated with a VoIPv6 dial-peer profile.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the **voice-class source interface** command is configured, the source address of Routing Table Protocol (RTP) generated by the gateway is taken from the address configured under the loopback interface. This command is used for policy-based routing (PBR) of voice packets originated by the gateway. The policy route map is configured under the loopback interface, and then the loopback interface is specified under the VoIP or VoIPv6 dial peer.

Examples

The following example associates a loopback interface with a VoIPv6 dial-peer profile:

```
Router(config)# dial-peer voice 1 voip
Router (config-dial-peer)# voice-class source interface loopback0
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice-class stun-usage

To configure voice class, enter voice class configuration mode called stun-usage and use the **voice-class stun-usage** command in global, dial-peer, ephone, ephone template, voice register pool, or voice register pool template configuration mode. To disable the voice class, use the **no** form of this command.

voice-class stun-usage *tag*

no voice-class stun-usage *tag*

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

The voice class is not defined.

Command Modes

Global configuration (config)
Dial peer configuration (config-dial-peer)
Ephone configuration (config-ephone)
Ephone template configuration (config-ephone-template)
Voice register pool configuration (config-register-pool)
Voice register pool template configuration (config-register-pool)

Command History

Release	Cisco Product	Modification
12.4(22)T	Cisco Unified CME 7.0	This command was introduced.
15.1(2)T	Cisco Unified CME 8.1	This command was modified. This command can be enabled in ephone summary, ephone template, voice register pool, or voice register pool template configuration mode.

Usage Guidelines

When the voice-class stun-usage is removed, the same is removed automatically from the dial-peer, ephone, ephone template, voice register pool, or voice register pool template configurations.

Examples

The following example shows how to set the **voice class stun-usage** tag to 10000:

```
Router(config)# voice class stun-usage 10000
Router(config-ephone)# voice class stun-usage 10000
Router(config-voice-register-pool)# voice class stun-usage 10000
```

Related Commands

Command	Description
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
stun flowdata agent-id	Configures the agent ID.

voice-class stun-usage (dial peer)

To enable firewall traversal for VoIP communications, use the **voice-class stun-usage** command in dial peer voice configuration mode. To disable firewall traversal, use the **no** form of this command.

voice-class stun-usage *tag*

no voice-class stun-usage *tag*

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

Firewall traversal is not enabled.

Command Modes

Dial-peer voice configuration (config-dial-peer).

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the voice-class stun-usage command is removed, the same is removed automatically from dial-peer configurations.

Examples

The following example shows how to set the **voice-class stun-usage** tag to 10.

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#voice-class stun-usage 10
```

Related Commands

Command	Description
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.

voice-class tone-signal

To assign a previously configured tone-signal voice class to a voice port, use the **voice-class tone-signal** command in voice-port configuration mode. To delete a tone-signal voice class, use the **no** form of this command.

voice-class tone-signal *tag*

no voice-class tone-signal *tag*

Syntax Description

tag	Unique label assigned to the voice class. The *tag* label maps to the tag label created using the **voice class tone-signal** global configuration command. Can be up to 32 alphanumeric characters.

Command Default Voice ports have no tone-signal voice class assigned.

Command Modes Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines The **voice-class tone-signal** command is available on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Note that the hyphenation in this command differs from the hyphenation used in a similar command, **voice class tone-signal**, which is used in global configuration mode.

Examples The following example assigns a previously configured voice class to voice port 1/1/0:

```
voice-port 1/0/0
 voice-class tone-signal mytones
```

Related Commands

Command	Description
voice class tone-signal	Enters voice-class configuration mode and assigns an identification tag number for a tone-signal voice class.

voice confirmation-tone

To disable the two-beep confirmation tone for private line, automatic ringdown (PLAR), or PLAR off-premises extension (OPX) connections, use the **voice confirmation-tone** command in voice-port configuration mode. To enable the two-beep confirmation tone, use the **no** form of this command.

voice confirmation-tone

no voice confirmation-tone

Syntax Description

This command has no arguments or keywords.

Command Default

The two-beep confirmation tone is heard on PLAR and PLAR OPX connections.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.

Usage Guidelines

Use this command to disable the two-beep confirmation tone that a caller hears when picking up the handset for PLAR and PLAR OPX connections. This command is valid only if the voice-port **connection** command is set to PLAR or PLAR OPX.

Examples

The following example disables the two-beep confirmation tone on voice port 1/0/0:

```
voice-port 1/0/0
 connection plar-opx
 voice confirmation-tone
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

voice dnis-map

To create or modify a Digital Number Identification Service (DNIS) map, use the **voice dnis-map** command in global configuration mode. To delete a DNIS map, use the **no** form of this command.

voice dnis-map *map-name* [*url*]

no voice dnis-map *map-name*

Syntax Description

map-name	Name of the DNIS map.
url	(Optional) URL of an external text file that contains a list of DNIS entries.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines A DNIS map is a table of DNIS numbers associated with a single dial peer. For applications such as VoiceXML, using a DNIS map makes it possible to configure a single dial peer for all DNIS numbers used to refer to VoiceXML documents. Keep the following considerations in mind when using voice DNIS maps.

- A separate entry must be made for each DNIS entry in a DNIS map. Wildcards are not supported.
- If a URL is not supplied, the command enters DNIS-map configuration mode, permitting the entry of DNIS numbers by using the **dnis** command.
- The URL argument points to the location of an external text file containing a list of DNIS entries (for example: tftp://dnismap.txt). This allows the administrator to maintain a single master file of all DNIS map entries, if desired, rather than configuring the DNIS entries on each gateway.

  The name of the text file extension is not significant; .doc, .txt, or .cfg are all acceptable because the extension is not checked. The entries in the file should look the same as a DNIS entry configured in Cisco IOS software (for example: dnis 5553305 url tftp://global/tickets/movies.vxml).
- External text files used for DNIS maps must be stored on TFTP servers; they cannot be stored on HTTP servers.
- To associate a DNIS map with a dial peer, use the **dnis-map** command.
- To view the configuration information for DNIS maps, use the **show voice dnis-map** command.

Examples

The following example shows how the **voice dnis-map** command is used to create a DNIS map:

```
voice dnis-map dmap1
```

The following example shows the **voice dnis-map** command used with a URL that specifies the location of a text file containing the DNIS entries:

```
voice dnis-map dmap2 tftp://keyer/dmap2/dmap2.txt
```

Following is an example of the contents of a text file comprising a DNIS map:

```
!Example dnis-map with 8 entries.
!
dnis 5550112 url tftp://global/ticket/vapptest1.vxml
dnis 5550111 url tftp://global/ticket/vapptest2.vxml
dnis 5550134 url tftp://global/ticket/vapptest3.vxml
dnis 5550178
dnis 5550100
dnis 5550101
dnis 5550102
dnis 5550103
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis-map	Associates a DNIS map with a dial peer.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map load	Reloads a DNIS map that has changed since the previous load.

voice dnis-map load

To reload a DNIS map that has been modified, use the **voice dnis-map load** command in privileged EXEC mode. This command does not have a **no** form.

voice dnis-map load *map-name*

Syntax Description

map-name	Name of the DNIS map to reload.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command reloads a DNIS map residing on an external server. Use this command when the DNIS map file has changed since the previous load.

To create or modify a DNIS map, use the **voice dnis-map** command.

Examples

The following example reloads a DNIS map named "mapfile1":

```
Router# voice dnis-map load mapfile1
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis-map	Associates a DNIS map with a dial peer.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map	Enters DNIS map configuration mode to create a DNIS map.

voice dsp crash-dump

To enable the crash dump feature and to specify the destination file and the file limit, enter the **voice dsp crash-dump** command in global configuration mode. To disable the feature, use the **no** form of the command.

voice dsp crash-dump [**destination** *url* | **file-limit** *limit-number*]

no voice dsp crash-dump

Syntax Description

destination *url*	Designates a valid file system where crash dump analysis is stored. The *url* argument must be set to a valid file system. The destination url can be one of the following • The file on a TFTP server with the following format: *tftp://x.x.x.x/subfolder/filename.* *The* x.x.x.x value is the IP address of the TFTP server • The file on the flashcard of the router, with the following format: *slot0:filename* **Note** The digital signal processor (DSP) crash dump feature is disabled when either the crash-dump destination is not specified.
file-limit *limit-number*	The crash dump **file-limit** keyword must be set to a non-zero value. The default is that the crash dump capability is turned off, as the *url* argument is empty, and the *file-number* argument is zero. The *limit-number* argument may range from 0 (no file will be written) to 99. **Note** The DSP crash dump feature is disabled when the crash-dump file limit is set to 0.

Command Default

Crash dump capability is turned off.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

To configure the router to write a crash dump file, the destination url in the **voice dsp crash-dump** command must be set to a valid file system, and the crash dump file limit must be set to a non-zero value. The default is that the crash dump capability is turned off, as the url field is empty, and the file limit is zero.

As each crash-dump file is created, the name of the file has a number appended to the end. This number is incremented from 1 to up to the file limit for each subsequent crash dump file written. If the router reloads, the number is reset back to 1, and so file number 1 is written again. After the file number reaches the maximum file limit, no more files are written.

The file count can be manually reset by setting the file limit to zero and then setting it to a non-zero limit. This has the effect of restarting the count of files written, causing the files 1 to the file limit of 99 to be able to be written again, thus overwriting the original files.

Setting the *file-number* argument to zero (the default) disables the collection of the dump from the DSP. In this case, the memory is not collected from the DSP, and the stack is not displayed on the console. If the keepalive mechanism detects a crashed DSP, the DSP is simply restarted.

Setting the *file-number* argument to a non-zero number but having a null destination url causes the dump to be collected and the stack to be displayed on the console, but no dump file is written.

If auto-recovery is turned off for the router, no DSP dump functions are enabled, no keepalive checks are done, and no dumps are collected or written.

Note Some types of flash need to be completely erased to free up space from deleted files, and some types of flash cannot have files overwritten with new versions until the entire flash is erased. As a result, you might want to set the file limit so that only one or two dump files are written to flash. This prevents flash from being filled up.

Note It is not recommended to write crash dump files to internal flash or bootflash, because these files are normally used to hold configuration information and Cisco IOS software images. Cisco recommends writing crash dump files to spare flash cards, which can be inserted into slot 0 or slot 1 on many of the routers. These cards usually do not hold critical information and may be erased. Additionally, these cards can be conveniently removed from the router and sent to Cisco, so that the crash dump files can be analyzed.

Examples

The following example enables the crash dump feature and specifies the destination file in slot 0:

```
Router configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# voice dsp crash-dump destination slot0:banjo-152-s

Router# end

1w0d:%SYS-5-CONFIG_I:Configured from console by console
```

Check your configuration by entering the show voice dsp crash-dump command in privileged EXEC configuration mode:

```
Router# show voice dsp crash-dump

Voice DSP Crash-dump status:
    Destination file url is slot0:banjo-152-s
File limit is 20
    Last DSP dump file written was
          tftp://112.29.248.12/tester/26-152-t2
    Next DSP dump file written will be slot0:banjo-152-s1
```

Related Commands

Command	Description
debug voice dsp crash-dump	Displays crash dump debug information.
show voice dsp crash-dump	Displays voice dsp crash dump information.

voice echo-canceller extended

To enable the extended G.168 echo canceller (EC) on the Cisco 1700 series, Cisco ICS7750, or Cisco AS5300, use the **voice echo-canceller extended** command in global configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1700 series and Cisco ICS 7750

voice echo-canceller extended

no voice echo-canceller extended

Cisco AS5300

voice echo-canceller extended [**codec small** *codec* **large** *codec*]

no voice echo-canceller extended

Syntax Description

codec	(Optional) Defines restricted codecs, both small and large.
small *codec*	Small footprint codec. Valid values for the *codec* argument are: • **g711** • **g726**
large *codec*	Large footprint codec. Valid values for the *codec* argument are: • **fax-relay** • **g723** • **g728** • **g729** • **gsmefr** • **gsmfr**

Command Default

V

Proprietary Cisco G.165 EC is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(3)	This command was modified to allow unrestricted codecs on the Cisco AS5300. The **codec** keyword was made optional.

Usage Guidelines

Cisco 1700 series and Cisco ICS7750

You do not have to shut down all the voice ports on the Cisco 1700 series or Cisco ICS7750 to switch the echo canceller, but you should make sure that when you switch the echo canceller, there are no active calls on the router.

Because echo cancellation is an invasive process that can minimally degrade voice quality, you should disable this command if it is not needed.

Cisco AS5300

This command is available only on the Cisco AS5300 with C542 or C549 digital signal processor module (DSPM) high-complexity firmware.

The **voice echo-canceller extended** command enables the extended EC on a Cisco AS5300 using C549 DSP firmware with one channel of voice per DSP and unrestricted codecs. Any codec is supported.

The **voice echo-canceller extended codec** command enables the extended EC on a Cisco AS5300 using C542 or C549 DSP firmware with two channels of voice per DSP and restricted codecs. Only specific codecs can be used with the extended EC.

If fax-relay is not selected as the large codec, the VoIP dial peer requires that you use the **fax rate disabled** command in dial peer configuration mode.

After choosing the codecs to be supported by the extended echo canceller, either remove all dial peers with different codecs not supported by your new configuration or modify the dial-peer codec selection by selecting a voice codec or fax-relay. When codecs are restricted, only one selection is allowed. You must have a VoIP dial peer configured with an extended EC-compatible codec to ensure voice quality on the connection.

This command is not accepted if there are active calls. If the EC is already in effect and a codec choice is changed, the system scans the dial peers. Any dial peers that do not conform to the new global command settings are changed, and the user is informed of the changes. Similarly, modem relay is incompatible with the extended EC and must be disabled globally for all dial peers.

Note This command is valid only when the **echo-cancel enable** command and the **echo-cancel coverage** command are enabled.

Examples

The following example sets the extended G.168 EC on the Cisco 1700 series or Cisco ICS7750:

```
Router(config)# voice echo-canceller extended
```

The following example sets the extended G.168 EC on the Cisco AS5300 with restricted codecs:

```
Router(config)# voice echo-canceller extended codec small g711 large g726
```

The following example shows an error message that displays when a restricted codec is not allowed:

```
Cannot configure now, dial-peer 8800 is configured with codec=g728, fax rate=disable,
modem=passthrough system.If necessary set this command to 'no', re-configure dial-peer
codec, fax rate and/or modem. Then re-enter this command.
```

In the above example, dial peer 8800 is misconfigured with a codec type, g728, that was not selected for the large codec type using the **voice echo-canceller extended** command.

Related Commands

Command	Description
echo-cancel coverage	Enables the cancellation of voice that is sent out the interface and is received on the same interface.
echo-cancel enable	Enables the cancellation of voice that is sent and received on the same interface.

voice enum-match-table

To create an ENUM match table for voice calls, use the **voice enum-match-table** in global configuration mode. To delete the ENUM match table, use the **no** form of this command.

voice enum-match-table *table-number*

no voice enum-match-table *table-number*

Syntax Description

table-number	Number of the ENUM match table. Range is from 1 to 15. There is no default value.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines The ENUM match table is a set of rules for matching incoming calls. When a call comes in, its called number is matched against the match pattern of the rule with the highest preference.

If it matches, the replacement pattern is applied to the number. The resulting number and the domain name of the rule are used to make an ENUM query.

If the called number does not match the match pattern, the next rule in order of preference is selected.

Examples The following example creates ENUM match table 3 for voice calls:

```
Router(config)# voice enum-match-table 3
Router(config-enum)# rule 1 5/(.*)/ /\1/e164.cisco.com
Router(config-enum)# rule 2 4/^9011\(.*\)/ /\1/e164.arpa
```

In this table, rule 1 matches any number. The resulting number is the same as the called number. That number and the domain name “e164.cisco.com” are used to make an ENUM query.

Rule 2 matches any number that starts with 9011. The 9011 is removed from the incoming number. The resulting number and the domain name “e164.arpa” are used for the ENUM query.

Suppose an incoming call has a called number of 4085551212. [Rule 2 is applied] first because it has a higher preference. The first few digits, 4085, do not match the 9011 pattern of rule 2, so [rule 1 is applied] next. The called number matches rule 1, and the resulting number is 4085551212. This number and “e164.cisco.com” form the ENUM query (2.1.2.1.5.5.5.8.0.4.e164.cisco.com).

Related Commands

Command	Description
rule (ENUM configuration)	Defines the matching, replacement, and rejection patterns for an ENUM match table.
show voice enum-match-table	Displays the configuration of voice ENUM match tables.
test enum	Tests the functionality of an ENUM match table.

voice hpi capture

To allocate the Host Port Interface (HPI) capture buffer size (in bytes) and to set up or change the destination URL for captured data, use the **voice hpi capture** command in global configuration mode. To stop all logging and file operations, to disable data transport from the capture buffer, and to automatically set the buffer size to 328, use the **no** form of this command.

voice hpi capture [**buffer** *size* | **destination** *url*]

no voice hpi capture buffer *size*

Syntax Description

buffer *size*	(Optional) Size of HPI capture buffer, in bytes. Range is from 328 to 9000000. The default is 328.
destination *url*	(Optional) Destination URL for storing captured data.

Command Default

328 bytes (no buffer is used if it is not configured explicitly)

Command Modes

Global configuration

Command History

Release	Modification
12.2(10)	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If you want to change the size of an existing non-zero buffer, you must first reset it to 0 and then change it from 0 to the new size.

The **destination** *url* option sets up or changes the destination URL for captured data. To disable data transport from the capture buffer, use the **no** form of the command. If the buffer is allocated, captured data is sent to the current URL (if it was already configured) until the new URL is specified.

If a new URL differs from the current URL and logging is enabled, the current URL is closed and all further data is sent to the new URL. Entering a blank URL or prefixing the command with **no** disables data transport from the capture buffer, and (if capture is enabled) captured data is stored in the capture buffer until it reaches its capacity.

Once the buffer-queueing program is running, the transport process attempts to connect to a new or existing "capture destination" URL. A version message is written to the URL, and if the message is successfully received, any further messages placed into the message queue are written to that URL. If a new URL is entered using the **voice hpi capture destination** *url* command, the open URL is closed, and the system attempts to write to the new URL. If the new URL does not work, the transport process exits. The transport process is restarted when another URL is entered or the system is restarted.

The **buffer** *size* option sets the maximum amount of memory (in bytes) that the capture system allocates for its buffers when it is active. The capture buffer is where the captured messages are stored before they are sent to the URL specified by the capture destination. The system is started by choosing the amount of memory (greater than 0 bytes) that the buffer-queueing system can allocate to the free message pool.

HPI messages can then be captured until buffer capacity is reached. Entering **0** for the buffer size and prefixing the command with **no** stops all logging and file operations and automatically sets the buffer size to 0.

The **voice hpi capture** command can be saved with the router configuration so that the command is active during router startup. This allows you to capture the HPI messages sent during router bootup before the CLI is enabled. After you have configured the buffer size in the running configuration (valid range is from 328 to 9000000), save it to the startup configuration using the **write** command or to the TFTP server using the **copy run tftp** command.

Caution Using the message logger feature in a production network environment impacts CPU and memory usage on the gateway.

Examples

The following example changes the size (in bytes) of the HPI capture buffer and initializes the buffer-queueing program:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# voice hpi capture buffer 40000

Router(config)# end
Router#

03:23:31:caplog:caplog_cli_interface:hpi capture buffer size set to 40000 bytes
03:23:31:caplog:caplog_logger_init:TRUE, Started task HPI Logger (PID 64)
03:23:31:caplog:caplog_cache_init:TRUE, malloc_named(39852), 123 elements (each 324 bytes
big)
03:23:31:caplog:caplog_logger_proc:Attempting to open ftp://172.23.184.233/c:b-38-117
03:23:32:%SYS-5-CONFIG_I:Configured from console by console
Router#
```

The following example sets the capture destination by entering a destination URL using FTP:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# voice hpi capture destination ftp://172.23.184.233/c:b-38-117a
Router(config)#

04:05:10:caplog:caplog_cli_interface:hpi capture
destination:ftp://172.23.184.233/c:b-38-117a
04:05:10:caplog:caplog_logger_init:TRUE, Started task HPI Logger (PID 19)
04:05:10:caplog:caplog_cache_init:Cache must be at least 324 bytes
04:05:10:caplog:caplog_logger_proc:Terminating...

Router(config)# end
Router#
```

Related Commands

Command	Description
debug hpi	Turns on the debug output for the logger.
show voice hpi capture	Displays the capture status and statistics.

voice hunt

To configure an originating or tandem router so that it continues dial-peer hunting if it receives a specified disconnect cause code from a destination router, use the **voice hunt** command in global configuration mode. To configure the router so that it stops dial-peer hunting if it receives a specified disconnect cause code (the default condition), use the **no** form of this command. To restore the default dial-peer hunt setting, use the **default** form of this command.

voice hunt {*disconnect-cause-code* | **all**}

no voice hunt {*disconnect-cause-code* | **all**}

default voice hunt

Syntax Description

disconnect-cause-code	A code returned from the destination router to indicate why an attempted end-to-end call was unsuccessful. If the specified disconnect cause code is returned from the last destination endpoint, dial peer hunting is enabled or disabled. Table 251 in the "Usage Guidelines" section describes the possible values. You can enter the keyword, decimal value, or hexadecimal value.
all	Continue dial-peer hunting for all disconnect cause codes returned from the destination endpoint.
default	Restores the default dial-peer hunt setting, that is, the router stops dial-peer hunting if it receives the user-busy or no-answer disconnect cause code.

Command Default

The router stops dial-peer hunting if it receives the user-busy or no-answer disconnect cause code.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced for VoFR on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810. It was also introduced for VoIP on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was implemented for VoIP on the Cisco AS5300 and Cisco AS5800.
12.0(7)XK	This command was implemented for VoIP on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T and implemented for VoIP on the Cisco MC3810.
12.1(3)XI	The **invalid-number** and **unassigned-number** keywords were added, and the command name was changed to **voice hunt**.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Release	Modification
12.2(4)T	Keywords were added for more disconnect cause codes.
12.3(8)T	The *disconnect-cause-code* argument was modified to accept nonstandard disconnect cause codes.

Usage Guidelines

This command is used with routers that act as originating or tandem nodes in a VoIP, VoFR, or Voice over ATM environment.

For an outgoing call from an originating VoIP gateway configured for rotary dial-peer hunting, more than one dial peer may match the same destination number. The matching dial peers may have different routes. After the voice call using the first dial peer gets disconnected, it will return a disconnect cause code. To have the router to pick up the next matching dial peer in the rotary group and set up a call, the router must be configure to continue hunting the various routes. Use this command to configure the router's hunting behavior when specified cause codes are received.

You can use this command to enable and disable dial-peer hunting when nonstandard disconnect cause codes are received. Nonstandard disconnect cause codes are those that are not defined in ITU-T Recommendation Q.931, but are used by service providers. When this command is used to disable dial-peer hunting for a specific disconnect cause code, it appears in the running configuration of the router.

The disconnect cause codes are described in Table 251. The decimal and hexadecimal value of the disconnect cause code follows the description of each possible keyword.

Table 251 Standard Disconnect Cause Codes

Keyword	Description	Decimal	Hex
access-info-discard	Access information discarded.	43	0x2b
all	Continue dial-peer hunting for all disconnect cause codes received from a destination router.		
b-cap-not-implemented	Bearer capability not implemented.	65	0x41
b-cap-restrict	Restricted digital information bearer capability only.	70	0x46
b-cap-unauthorized	Bearer capability not authorized.	57	0x39
b-cap-unavail	Bearer capability not available.	58	0x3a
call-awarded	Call awarded.	7	0x7
call-cid-in-use	Call exists, call ID in use.	83	0x53
call-clear	Call cleared.	86	0x56
call-reject	Call rejected.	21	0x15
cell-rate-unavail	Cell rate not available.	37	0x25
channel-unacceptable	Channel unacceptable.	6	0x6
chantype-not-implement	Channel type not implemented.	66	0x42
cid-in-use	Call ID in use.	84	0x54
codec-incompatible	Codec incompatible.	171	0xab
cug-incalls-bar	Closed user group (CUG) incoming calls barred.	55	0x37
cug-outcalls-bar	CUG outgoing calls barred.	53	0x35

Table 251 Standard Disconnect Cause Codes (continued)

Keyword	Description	Decimal	Hex
dest-incompatible	Destination incompatible.	88	0x58
dest-out-of-order	Destination out of order.	27	0x1b
dest-unroutable	No route to destination.	3	0x3
dsp-error	Digital signal processor (DSP) error.	172	0xac
dtl-trans-not-node-id	Designated transit list (DTL) transit not my node ID.	160	0xa0
facility-not-implemented	Facility not implemented.	69	0x45
facility-not-subscribed	Facility not subscribed.	50	0x32
facility-reject	Facility rejected.	29	0x1d
glare	Glare.	15	0xf
glaring-switch-pri	Glaring switch PRI.	180	0xb4
htspm-oos	Holst Telephony Service Provider Module (HTSPM) out of service.	129	0x81
ie-missing	Mandatory information element missing.	96	0x60
ie-not-implemented	Information element not implemented.	99	0x63
info-class-inconsistent	Inconsistency in information and class.	62	0x3e
interworking	Interworking.	127	0x7f
invalid-call-ref	Invalid call reference value.	81	0x51
invalid-ie	Invalid information element contents.	100	0x64
invalid-msg	Invalid message.	95	0x5f
invalid-number	Invalid number.	28	0x1c
invalid-transit-net	Invalid transit network.	91	0x5b
misdialled-trunk-prefix	Misdialed trunk prefix.	5	0x5
msg-incomp-call-state	Message in incomplete call state.	101	0x65
msg-not-implemented	Message type not implemented.	97	0x61
msgtype-incompatible	Message type not compatible.	98	0x62
net-out-of-order	Network out of order.	38	0x26
next-node-unreachable	Next node unreachable.	128	0x80
no-answer	No user answer.	19	0x13
no-call-suspend	No call suspended.	85	0x55
no-channel	Channel does not exist.	82	0x52
no-circuit	No circuit.	34	0x22
no-cug	Nonexistent CUG.	90	0x5a
no-dsp-channel	No DSP channel.	170	0xaa
no-req-circuit	No requested circuit.	44	0x2c
no-resource	No resource.	47	0x2f
no-response	No user response.	18	0x12

Table 251 Standard Disconnect Cause Codes (continued)

Keyword	Description	Decimal	Hex
no-voice-resources	No voice resources available.	126	0x7e
non-select-user-clear	Nonselected user clearing.	26	0x1a
normal-call-clear	Normal call clearing.	16	0x10
normal-unspecified	Normal, unspecified.	31	0x1f
not-in-cug	User not in CUG.	87	0x57
number-changeed	Number changed.	22	0x16
param-not-implemented	Nonimplemented parameter passed on.	103	0x67
perm-frame-mode-oos	Permanent frame mode out of service.	39	0x27
perm-frame-mode-oper	Permanent frame mode operational.	40	0x28
precedence-call-block	Precedence call blocked.	46	0x2e
preempt	Preemption.	8	0x8
preempt-reserved	Preemption reserved.	9	0x9
protocol-error	Protocol error.	111	0x6f
qos-unavail	QoS unavailable.	49	0x31
rec-timer-exp	Recovery on timer expiry.	102	0x66
redirect-to-new-destination	Redirect to new destination.	23	0x17
req-vpci-vci-unavail	Requested VPCI VCI not available.	35	0x23
send-infotone	Send information tone.	4	0x4
serv-not-implemented	Service not implemented.	79	0x4f
serv/opt-unavail-unspecified	Service or option not available, unspecified.	63	0x3f
stat-enquiry-resp	Response to status enquiry.	30	0x1e
subscriber-absent	Subscriber absent.	20	0x14
switch-congestion	Switch congestion.	42	0x2a
temp-fail	Temporary failure.	41	0x29
transit-net-unroutable	No route to transit network.	2	0x2
unassigned-number	Unassigned number.	1	0x1
unknown-param-msg-discard	Unrecognized parameter message discarded.	110	0x6e
unsupported-aal-parms	ATM adaptation layer (AAL) parameters not supported.	93	0x5d
user-busy	User busy.	17	0x11
vpci-vci-assign-fail	Virtual path connection identifier virtual channel identifier (VPCI VCI) assignment failure.	36	0x24
vpci-vci-unavail	No VPCI VCI available.	45	0x2d

Examples

The following example configures the originating or tandem router to continue dial-peer hunting if it receives a user-busy disconnect cause code from a destination router:

```
voice hunt user-busy
```

The following example configures the originating or tandem router to continue dial-peer hunting if it receives an invalid-number disconnect cause code from a destination router:

```
voice hunt 28
```

The following example configures the originating or tandem router to continue dial-peer hunting if it receives a facility-not-subscribed disconnect cause code from a destination router:

```
voice hunt 0x32
```

Related Commands

Command	Description
huntstop	Disables all further dial-peer hunting if a call fails when using hunt groups.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.

voice iec syslog

To enable viewing of Internal Error Codes as they are encountered in real time, use the **voice iec syslog** command in global configuration mode. To disable IEC syslog messages, use the **no** form of this command.

voice iec syslog

no voice iec syslog

Syntax Description

This command has no arguments or keywords.

Command Default

IEC syslog messages are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example enables IEC syslog messages:

```
router(config)# voice iec syslog
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics iec	Displays iec statistics
show voice statistics interval-tag	Displays interval options available for IEC statistics
voice statistics type iec	Enables collection of IEC statistics

voice local-bypass

To configure local calls to bypass the digital signal processor (DSP), use the **voice local-bypass** command in global configuration mode. To direct local calls through the DSP, use the **no** form of this command.

voice local-bypass

no voice local-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

Local calls bypass the DSP.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced.
12.0(7)XK	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Local calls (calls between voice ports on a router or concentrator) normally bypass the DSP to minimize use of system resources. Use the **no** form of the **voice local-bypass** command if you need to direct local calls through the DSP. Input gain and output attenuation can be configured only if calls are directed through the DSP.

Examples

The following example configures a Cisco router to pass local calls through the DSP:

```
no voice local-bypass
```

Related Commands

Command	Description
input gain	Configures a specific input gain value.
output attenuation	Configures a specific output attenuation value.

voice mlpp

To enter MLPP configuration mode to enable MLPP service, use the voice service command in global configuration mode. To disable MLPP service, use the **no** form of this command.

voice mlpp

no voice mlpp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Voice-mlpp configuration mode is used for the gateway globally.

Examples

The following example shows how to enter voice-mlpp configuration mode:

```
Router(config)# voice mlpp
Router(config-voice-mlpp)# access-digit
```

Related Commands

Command	Description
access-digit	Defines the access digit that phone users dial to request a precedence call.
mlpp preemption	Enables calls on an SCCP phone or analog FXS port to be preempted.
preemption trunkgroup	Enables preemption capabilities on a trunk group.

voicemail (stcapp-fsd)

To designate an SCCP telephony control (STC) application feature speed-dial code to speed dial the voice-mail number, use the **voicemail** command in STC application feature speed-dial configuration mode. To return the code to its default, use the **no** form of this command.

voicemail *keypad-character*

no voicemail

Syntax Description

keypad-character	One or two digits that can be dialed on a telephone keypad. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 0 (zero) for one-digit codes; 00 (two zeroes) for two-digit codes. **Note** Number of digits depends on the value set with the **digit** command.

Command Default

The default voice-mail code is 0 (zero) for one-digit codes; 00 (two zeros) for two-digit codes.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	The *keypad-character* argument was modified to allow two-digit codes.

Usage Guidelines

This command is used with the STC application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

To use the speed-dial to voice-mail feature on a phone, dial the feature speed-dial (FSD) prefix and the code that has been configured with this command (or the default if this command was not used). For example, if the FSD prefix is * (the default), and you want to dial the voice-mail phone number, dial *0.

Note that the number that will be speed-dialed for voice mail must be set on Cisco CallManager or the Cisco CallManager Express system.

This command is reset to its default value if you modify the value of the **digit** command. For example, if you set the **digit** command to 2, then change the **digit** command back to its default of 1, the voice-mail FSD code is reset to 0 (zero).

If you set this code to a value that is already in use for another FSD code, you receive a warning message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

The **show running-config** command displays nondefault FSD codes only. The **show stcapp feature codes** command displays all FSD codes.

Examples

The following example sets an FSD prefix of two pound signs (##) and a voice-mail code of 8. After these values have been configured, a phone user presses ##8 to dial the voice-mail number.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ##
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for STC application feature speed-dial codes.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature codes.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.

voiceport

To enable a private line automatic ringdown (PLAR) connection for an analog phone, use the **voiceport** command in SCCP PLAR configuration mode. To remove PLAR from the voice port, use the **no** form of this command.

voiceport *port-number* **dial** *dial-string* [**digit** *dtmf-digits* [**wait-connect** *wait-msecs*] [**interval** *inter-digit-msecs*]]

no voiceport *port-number*

Syntax Description

port-number	Analog foreign exchange station (FXS) voice port number. Range: 2/0 to 2/23.
dial *dial-string*	String of up to 16 characters that can be dialed on a telephone keypad. Valid characters are 0 through 9, A through D, an * (asterisk) and # (pound sign). The voice gateway sends this string to the call-control system when the analog phone goes off hook.
digit *dtmf-digits*	(Optional) String of up to 16 characters that can be dialed on a telephone keypad. Valid characters are 0 through 9, A through D, an * (asterisk), # (pound sign), and comma (,). The voice gateway sends this string to the call-control system after the *wait-msecs* expires. Each comma represents a one second wait.
wait-connect *wait-msecs*	(Optional) Number of milliseconds that the voice gateway waits after voice cut-through before out-pulsing the DTMF digits. Range: 0 to 30000, in multiples of 50. Default: 50. If 0, DTMF digits are sent automatically by voice gateway after call is connected.
interval *inter-digit-msecs*	(Optional) Number of milliseconds between the DTMF digits. Range: 50 to 500, in multiples of 50. Default: 50.

Command Default

Disabled (PLAR is not set for the voice port).

Command Modes

SCCP PLAR configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command enables PLAR on analog FXS ports that use Skinny Client Control Protocol (SCCP) for call control. If the **digit** keyword is not used, DTMF digits are not out-pulsed; the voice port uses a simple PLAR connection and the other keywords are not available.

Voice ports can be configured in any order. For example, you can configure port 2/23 before port 2/0. The **show running-config** command lists the ports in ascending order.

Before a PLAR port can become operational, the STC application must first be enabled in the corresponding dial-peer using the **service stcapp** command. If you configure a port for PLAR before enabling the STC application in the dial peer you receive a warning message.

PLAR phones support most of the same features as normal analog phones. The PLAR phone handles incoming calls and supports hookflash for basic supplementary features such as call transfer, call waiting, and conference. The PLAR phone does not support other features such as call forwarding, redial, speed dial, call park, call pick up from a PLAR phone, AMWI, or caller ID.

Examples

The following example enables the PLAR feature on port 2/0, 2/1, and 2/3. When a phone user picks up the handset on the analog phone connected to port 2/0, the system automatically rings extension 3660 and after waiting 500 milliseconds, dials 1234. The DTMF digits are out-pulsed to the destination port at an interval of 200 milliseconds.

```
Router(config)# sccp plar
Router(config-sccp-plar)# voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
Router(config-sccp-plar)# voiceport 2/1 dial 3264 digit 678,,,9*0,,#123 interval 100
Router(config-sccp-plar)# voiceport 2/3 dial 3478 digit 34567 wait-connect 500
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and defines a dial peer.
sccp plar	Enters SCCP PLAR configuration mode.

voice-port

To enter voice-port configuration mode, use the **voice-port** command in global configuration mode.

Cisco 1750 and Cisco 1751

voice-port *slot-number/port*

Cisco 2600 series, Cisco 3600 Series, and Cisco 7200 Series

voice-port {*slot-number/subunit-number/port* | *slot/port*:*ds0-group-no*}

Cisco 2600 and Cisco 3600 Series with a High-Density Analog Network Module (NM-HDA)

voice-port {*slot-number/subunit-number/port*}

Cisco AS5300

voice-port *controller-number*:**D**

Syntax Description

Cisco 1750 and Cisco 1751

slot-number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed.
port	Voice port number. Valid entries are 0 and 1.

Cisco 2600 series, Cisco 3600 Series, and Cisco 7200 Series

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
port	Voice port number. Valid entries are 0 and 1.
slot	The router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
port:	Indicates the voice interface card location. Valid entries are 0 and 3.
ds0-group-no	Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

Cisco AS5300:

controller-number	T1 or E1 controller.
:D	D channel associated with ISDN PRI.

Command Default

No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(3)T	This command was implemented on the Cisco 2600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(7)T	This command was implemented on the Cisco AS5800, Cisco 7200 series, and Cisco 1750. Arguments were added for the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was implemented on Cisco 1751 and Cisco 1760. This command was modified to accommodate the additional ports of the NM-HDA on the Cisco 2600 series, Cisco 3640, and Cisco 3660.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.

Usage Guidelines Use the **voice-port** global configuration command to switch to voice-port configuration mode from global configuration mode. Use the **exit** command to exit voice-port configuration mode and return to global configuration mode.

Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5300.

Examples The following example accesses voice-port configuration mode for port 0, located on subunit 0 on a VIC installed in slot 1:

```
voice-port 1/0/0
```

The following example accesses voice-port configuration mode for a Cisco AS5300:

```
voice-port 1:D
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice encapsulation.

voice-port (MGCP profile)

The **voice-port** (MGCP profile) command is replaced by the **port** (MGCP profile) command in Cisco IOS Release 12.2(8)T. See the **port** (MGCP profile) command for more information.

voice-port busyout

To place all voice ports associated with a serial or ATM interface into a busyout state, use the **voice-port busyout** command in interface configuration mode. To remove the busyout state on the voice ports associated with this interface, use the **no** form of this command.

voice-port busyout

no voice-port busyout

Syntax Description

This command has no arguments or keywords.

Command Default

The voice ports on the interface are not in busyout state.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on Cisco MC3810.

Usage Guidelines

This command busies out all voice ports associated with the interface, except any voice ports configured to busy out under specific conditions using the **busyout monitor** and **busyout seize** commands.

Examples

The following example places the voice ports associated with serial interface 1 into busyout state:

```
interface serial 1
 voice-port busyout
```

The following example places the voice ports associated with ATM interface 0 into busyout state:

```
interface atm 0
 voice-port busyout
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port into the busyout monitor state.
busyout seize	Changes the busyout action for an FXO or FXS voice port.
show voice busyout	Displays information about the voice busyout state.

voice rtp send-recv

To establish a two-way voice path when the Real-Time Transport Protocol (RTP) channel is opened, use the **voice rtp send-recv command in** global configuration mode. To reset to the default, use the **no** form of this command.

voice rtp send-recv

no voice rtp send-recv

Syntax Description

This command has no arguments or keywords.

Command Default

The voice path is cut-through in only the backward direction when the RTP channel is opened.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on Cisco 2600, Cisco 3600, Cisco 7200, Cisco 7500, Cisco AS5300, Cisco AS5800, and Cisco MC3810 platforms.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command should be enabled only when the voice path must be cut-through (established) in both the backward and forward directions before a Connect message is received from the destination switch. This command affects all VoIP calls when it is enabled.

Examples

The following example enables the voice path to cut-through in both directions when the RTP channel is opened:

```
voice rtp send-recv
```

voice-service dsp-reservation

To specify the percentage of DSP resources that are reserved strictly for VOIP on the voice card, use the **voice-service dsp-reservation** command in voice-card configuration. To reset the percentage of DSP resources, use the **no** form of this command.

voice-service-dsp reservation *percentage*

no voice-service-dsp reservation *percentage*

Syntax Description

percentage	Percentage of DSP resources on this voice card that are reserved for voice services. The remaining DSP resources will be available for video services.

Defaults

The default voice reservation is 100%.

Command Modes

voice-card configuration (config-voicecard)

Command History

Release	Modification
15.1(4)M	The command was introduced.

Usage Guidelines

Use this command to reserve a percentage of the voice card for voice services. The remaining DSP resources will be used for video services. A reservation of 100% specified that all DSP resources will be used for voice services.

Note You can configure a percentage less than 100% only when there is a video license and the appropriate PVDM# modules are installed.

Tip DSP can become fragmented when you change the percentage of DSP resources reserved for voice services when there are TDM voice or DSP farm profiles configured. To ensure the best system performance, reload the router when you change the **voice-service-dsp-reservation**.

Examples

The following example enters voice-card configuration mode and sets the percentage of DSP resources for voice to 60%:

```
Router(config)# voice card 0
Router(config-voicecard)# voice-service dsp-reservation 60
```

Related Commands

Command	Description
dspfarm profile	Adds the specified voice card to those participating in a DSP resource pool.

voice service

To enter voice-service configuration mode and to specify a voice-encapsulation type, use the **voice service** command in global configuration mode.

voice service {**pots** | **voatm** | **vofr** | **voip**}

Syntax Description

pots	Telephony voice service.
voatm	Voice over ATM (VoATM) encapsulation.
vofr	Voice over Frame Relay (VoFR) encapsulation.
voip	Voice over IP (VoIP) encapsulation.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T for VoIP on the Cisco 2600 series and the Cisco 3600 series.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines Voice-service configuration mode is used for packet telephony service commands that affect the gateway globally.

Examples The following example enters voice-service configuration mode for VoATM service commands:

```
voice service voatm
```

voice source-group

To define a source IP group for voice calls, use the **voice source-group** command in global configuration mode. To delete the source IP group, use the **no** form of this command.

voice source-group *name*

no voice source-group *name*

Syntax Description

name	Name of the IP group. Maximum length of the source IP group name is 31 alphanumeric characters.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **voice source-group** command to assign a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call.

Carrier IDs and trunk group labels must not have the same names.

Do not mix carrier IDs and trunk group labels within a source IP group.

A terminating gateway can be configured with carrier ID source IP groups and trunk-group-label source IP groups. The name of the source IP group must be unique to the gateway.

Examples The following example initiates source IP group "utah2" for VoIP calls:

```
Router(config)# voice source-group utah2
```

Related Commands

Command	Description
access-list	Defines a list of source groups for identifying incoming calls.
carrier-id (voice source group)	Specifies the carrier handling a VoIP call.
description (voice source group)	Assigns a disconnect cause to a source IP group.
h323zone-id (voice source group)	Assigns a zone ID to an incoming H.323 call.
translation-profile (source group)	Assigns a translation profile to a source IP group.
trunk-group-label (voice source group)	Specifies the trunk handling a VoIP call.

voice statistics accounting method

To enable voice accounting statistics to be collected for a specific accounting method list and to specify the pass criteria for call legs, use the **voice statistics accounting method** command in global configuration mode. To disable the collection of statistics for the accounting method, use the **no** form of this command.

voice statistics accounting method *method-list-name* **pass** {**start-interim-stop** | **start-stop** | **stop-only**}

no voice statistics accounting method *method-list-name* **pass** {**start-interim-stop** | **start-stop** | **stop-only**}

Syntax Description

method-list-name	Name of the accounting method list. The *method-list-name* argument is the same as that configured using the **method** command in gateway accounting AAA configuration mode.
pass	The pass criteria for call legs (PSTN or IP) and call directions (inbound or outbound) that is used by the method list. **Note** The definition of pass implies that all start, stop, or interim messages are acknowledged by the designated servers. The definition of failure implies that any start, stop, or interim message is rejected or is timed out by the designated servers.
start-interim-stop	All start, interim, and stop pass criteria records are counted.
start-stop	All start and stop pass criteria records are counted.
stop-only	Only stop pass criteria records are counted.

Command Default

No statistics for the specified accounting method list are collected.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows that h323 is specified as the method list and that the pass criterion is stop-only:

```
Router(config)# voice statistics accounting method h323 pass stop-only
```

Related Commands

Command	Description
method	Specifies the AAA method list name to be used.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.

Command	Description
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics display-format separator

To configure the display format of the statistics on the gateway, use the **voice statistics display-format separator** command in global configuration mode. To return the display format of the statistics to the default value, use the **no** form of this command.

voice statistics display-format separator {**space** | **tab** | **new-line** | **char** *char*}

no voice statistics display-format separator {**space** | **tab** | **new-line** | **char** *char*}

Syntax Description

separator	Type of separator used in the displayed format.
space	A space is used for the formatting between each statistic in the displayed output.
tab	A tab is used for the formatting between each statistic in the displayed output.
new-line	A new line is used for the formatting between each statistic in the displayed output.
char *char*	A character is used for the formatting between each statistic in the displayed output. The *char* argument is a visible ASCII character used for the formatting between each statistic in the displayed output.

Command Default

A comma (,) is the default separator.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows that a space is specified as the display separator:

```
Router(config)# voice statistics display-format separator space
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.

Command	Description
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics field-params

To configure the parameters of call statistics fields on the gateway, use the **voice statistics field-params** command in global configuration mode. To return the call statistics parameters to the default values, use the **no** form of this command.

voice statistics field-params {**mcd** *value* | **lost-packet** *value* | **packet-latency** *value* | **packet-jitter** *value*}

no voice statistics field-params {**mcd** *value* | **lost-packet** *value* | **packet-latency** *value* | **packet-jitter** *value*}

Syntax Description

mcd	Minimum call duration. The *value* argument is an integer that represents the number of milliseconds. Valid values are from 0 to 30. The default is 2.
lost-packet	Lost voice packet threshold. The *value* argument is an integer that represents milliseconds. Valid values are from 0 to 65535. The default is 1000.
packet-latency	Voice packet latency threshold. The *value* argument is an integer that represents milliseconds. Valid values are from 0 to 500. The default is 250.
packet-jitter	Voice packet jitter threshold. The *value* argument is an integer that represents milliseconds. Valid values are from 0 to 1000. The default is 250.

Command Default

MCD is 2 milliseconds.
Lost packet threshold is 1000 milliseconds.
Packet latency threshold is 250 milliseconds.
Packet jitter threshold is 250 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example configures a minimum call duration of 5 milliseconds:

```
Router(config)# voice statistics field-params mcd 5
```

The following example configures a lost packet threshold of 250 milliseconds:

```
Router(config)# voice statistics field-params lost-packet 250
```

The following example configures a packet-latency threshold of 300 milliseconds:

```
Router(config)# voice statistics field-params packet-latency 300
```

The following example configures a packet-jitter threshold of 245 milliseconds:

```
Router(config)# voice statistics field-params packet-jitter 245
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics max-storage-duration

To configure the maximum amount of time for which collected statistics are stored in the system memory of the gateway, use the **voice statistics max-storage-duration** command in global configuration mode. To remove the configured maximum storage duration, use the **no** form of this command.

voice statistics max-storage-duration {**day** *value* | **hour** *value* | **minute** *value*}

no voice statistics max-storage-duration {**day** *value* | **hour** *value* | **minute** *value*}

Syntax Description

day *value*	Number of days for which call statistics data are to be stored. The *value* argument has a valid range from 0 to 365.
hour *value*	Number of hours for which call statistics data are to be stored. The *value* argument has a valid range from 0 to 720.
minute *value*	Number of minutes for which call statistics data are to be stored. The *value* argument has a valid range from 0 to 1440.

Command Default

If no length of time is configured, no memory is allocated for those call statistic records that have stopped after the end of their collection intervals. If no memory is allocated, only active call statistic record buffers are kept in system memory.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The maximum storage duration means the time-to-exist duration of the call statistic records on the gateway.

The values entered using this command also apply to the collection of VoIP internal error codes (IECs).

Examples

The following example shows that the maximum storage duration for the collection of voice call statistics has been set for 60 minutes:

```
Router(config)# voice statistics max-storage-duration minute 60
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics push

To configure the method for pushing signaling statistics, VoIP AAA accounting statistics, or Cisco internal error codes (IECs) to an FTP or syslog server, use the **voice statistics push** command in global configuration mode. To disable the configured push method, use the **no** form of this command.

voice statistics push {**ftp url** *ftp-url* [**max-file-size** *value*]} | {**syslog** [**max-msg-size** *value*]}

no voice statistics push {**ftp url** *ftp-url* [**max-file-size** *value*]} | {**syslog** [**max-msg-size** *value*]}

Syntax Description

ftp url *ftp-url*	URL of the FTP server to which voice statistics are to be pushed. The syntax of the *ftp-url* argument follows: ftp://user:password@host:port//directory1/directory2
max-file-size *value*	(Optional) Maximum size of a voice statistics file to be pushed to an FTP server, in bytes. The valid range of the *value* argument is from 1024 to 4294967296. The default value is 400000000 (4 GB).
syslog	Voice statistics are pushed to a syslog server.
max-msg-size *value*	(Optional) Maximum size of a voice statistics file to be pushed to a syslog server, in bytes. The valid range of the *value* argument is from 1024 to 4294967296. The default value is 400000000 (4 GB).

Command Default

Voice statistics are not pushed to an FTP or syslog server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The gateway configuration should be consistent with the configuration on the FTP or syslog servers. This command may also be used to push Cisco VoIP internal error codes (IECs) to either an FTP server or a syslog server.

Examples

The following is a configuration example showing a specified FTP server and maximum file size:

```
Router(config)# voice statistics push ftp url ftp://john:doe@abc:23//directory1/directory2
max-file-size 10000
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics time-range

To specify a time range to collect statistics from the gateway on a periodic basis, since the last reset, or for a specific time duration , use the **voice statistics time-range** command in global configuration mode. To disable the time-range settings, use the **no** form of this command.

Statistics Collection on a Periodic Basis

voice statistics time-range periodic *interval* **start** *hh*:*mm* {**days-of-week** *{*Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday | daily | weekdays | weekend*}} [*end *hh*:*mm {*days-of-week *{*Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday*}}]*

no voice statistics time-range periodic *interval* **start** *hh*:*mm* {**days-of-week** *{*Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday | daily | weekdays | weekend*}} [*end *hh*:*mm {*days-of-week *{*Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday*}}]*

Statistics Collection Since the Last Reset or Reboot of the Gateway

voice statistics time-range since-reset

no voice statistics time-range since-reset

Statistics Collection at a Specific Time Duration

voice statistics time-range specific start *hh*:*mm day month year end hh*:*mm day month year*

no voice statistics time-range specific start *hh*:*mm day month year end hh*:*mm day month year*

Syntax Description

Statistics Collection on a Periodic Basis:	
periodic	Call statistics are collected for a configured period.
interval	Specifies the periodic interval during which statistics will be collected. Valid entries for this value are **5minutes**, **15minutes**, **30minutes**, **60minutes**, or **1day**.
start/end	Specifies the start and ending periods of the statistics collection. If no end time is entered, then the statistics collection continues nonstop. By default, there is no end of the collection period.
hh:mm	Specifies the start and ending times for the periodic statistics collection in hours and minutes. The times entered must be in 24-hour format.
days-of-week	Specifies the start and ending days of the week that call statistics are collected. You can configure a specific day of the week, or one of the following: • **daily**—Call statistics are collected daily. • **weekdays**—Call statistics are collected on weekdays only. • **weekend**—Call statistics are collected on weekends only. The default value is **daily**.

Statistics Collection Since the Last Reset or Reboot of the Gateway	
since-reset	Call statistics are collected only since a reset or reboot of the gateway. **Note** Voice statistics collection on the gateway is reset using the **clear voice statistics csr** command.
Statistics Collection at a Specified Time Duration:	
specific	Call statistics are collected for a specific time duration.
start/end	Specifies the start and end times of the statistics collection. The required arguments for both the **start** and **end** keywords are as follows: • *hh***:***mm*—Hour and minute. The times entered must be in 24-hour format. • *day*—Day of the month. Valid values are from 1 to 31. • *month*—Month for the statistics collection to start. Enter the month name, for example, January, or February. The default is the current month. • *year*—Year. Valid values are from 1993 to 2035. The default is the current year.

No statistics are collected by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

There should be only one specific or periodic configuration at any one time. If a second specific or periodic configuration is configured, the request is rejected and a warning message displays. If the **no** form of the command is used during the specific time range, the corresponding collection will stop and FTP or syslog messages will not be sent.

Examples

The following example shows that the time range is periodic and set to collect statistics for a 60-minute period on weekdays only beginning at 12:00 a.m.:

```
Router(config)# voice statistics time-range periodic 60minutes start 12:00 days-of-week
weekdays
```

The following example configures the gateway to collect call statistics since the last reset (specified with the **clear voice statistics csr** command) or since the last time the gateway was rebooted:

```
Router(config)# voice statistics time-range since-reset
```

The following example configures the gateway to collect statistics from 10:00 a.m. on the first day of January to 12:00 a.m. on the second day of January:

```
Router(config)# voice statistics time-range specific start 10:00 1 January 2004 end 12:00
2 January 2004
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics type csr

To configure a gateway to collect VoIP AAA accounting statistics or voice signaling statistics, independently or at the same time, use the **voice statistics type csr** command in global configuration mode. To disable the counters, use the **no** form of this command.

voice statistics type csr [**accounting** | **signaling**]

no voice statistics type csr [**accounting** | **signaling**]

Syntax Description

accounting	(Optional) VoIP AAA accounting statistics are collected.
signaling	(Optional) Voice signaling statistics are collected.

Command Default No accounting or signaling call statistics records (CSRs) are collected on the gateway.

Command Modes Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines If you do not specify a keyword, both accounting and signaling CSRs are collected. Accounting and signaling CSR collection can be enabled and disabled independently.

Examples The following example shows that both types of CSRs will be collected:

```
Router(config)# voice statistics type csr
```

The following example enables accounting CSRs to be collected:

```
Router(config)# voice statistics type csr accounting
```

The following example enables signaling CSRs to be collected:

```
Router(config)# voice statistics type csr signaling
```

The following example disables the collection of both signaling and accounting CSRs:

```
Router(config)# no voice statistics type csr
```

The following example disables the collection of signaling CSRs only:

```
Router(config)# no voice statistics type csr signaling
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time range	Specifies the time range to collect CSRs.

voice statistics type iec

To enable collection of Internal Error Code (IEC) statistics, use the **voice statistics type iec** command in global configuration mode. To disable IEC statistics collection, use the **no** form of this command.

voice statistics type iec

no voice statistics type iec

Syntax Description

This command has no arguments or keywords.

Command Default

IEC statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example enables IEC statistics collection:

```
router(config)# voice statistics type iec
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics	Displays voice statistics
show voice statistics interval-tag	Displays interval options available for IEC statistics
voice statistics time-range since-reset	Enables collection of call statistics accumulated since the last resetting of IEC counters

voice translation-profile

To define a translation profile for voice calls, use the **voice translation-profile** command in global configuration mode. To delete the translation profile, use the **no** form of this command.

voice translation-profile *name*

no voice translation-profile *name*

Syntax Description

name	Name of the translation profile. Maximum length of the voice translation profile name is 31 alphanumeric characters.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines After translation rules are defined, they are grouped into profiles. The profiles collect a set of rules that, taken together, translate the called, calling, and redirected numbers in specific ways. Up to 1000 profiles can be defined. Each profile must have a unique name.

These profiles are referenced by trunk groups, dial peers, source IP groups, voice ports, and interfaces for handling call translations.

Examples The following example initiates translation profile “westcoast” for voice calls. The profile uses translation rules 1, 2, and 3 for various types of calls.

```
Router(config)# voice translation-profile westcoast
Router(cfg-translation-profile)# translate calling 2
Router(cfg-translation-profile)# translate called 1
Router(cfg-translation-profile)# translate redirect-called 3
```

Related Commands

Command	Description
rule (voice translation-rule)	Defines call translation criteria.
show voice translation-profile	Displays one or more translation profiles.
translate (translation profiles)	Associates a translation rule with a voice translation profile.

voice translation-rule

To define a translation rule for voice calls, use the **voice translation-rule** command in global configuration mode. To delete the translation rule, use the **no** form of this command.

voice translation-rule *number*

no voice translation-rule *number*

Syntax Description

number	Number that identifies the translation rule. Range is from1 to 2147483647.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **voice translation-rule** command to create the definition of a translation rule. Each definition includes up to 15 rules that include SED-like expressions for processing the call translation. A maximum of 128 translation rules are supported.

These translation rules are grouped into profiles that are referenced by trunk groups, dial peers, source IP groups, voice ports, and interfaces.

Examples

The following example initiates translation rule 150, Which includes two rules:

```
Router(config)# voice translation-rule 150
Router(cfg-translation-rule)# rule 1 reject /^408\(.(\)/
Router(cfg-translation-rule)# rule 2 /\(^...\)853\(...\)/ /\1525\2/
```

Related Commands

Command	Description
rule (voice translation-rule)	Defines the matching, replacement, and rejection patterns for a translation rule.
show voice translation-rule	Displays the configuration of a translation rule.

voice vad-time

To change the minimum silence detection time for voice activity detection (VAD), use the **voice vad-time** command in global configuration mode. To reset to the default, use the **no** form of this command.

voice vad-time *milliseconds*

no voice vad-time

Syntax Description

milliseconds	Waiting period, in milliseconds, before silence detection and suppression of voice-packet transmission. Range is from 250 to 65536. The default is 250.

Command Default

250 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command affects all voice ports on a router or concentrator, but it does not affect calls already in progress.

You can use this command in transparent common-channel signaling (CCS) applications in which you want VAD to activate when the voice channel is idle, but not during active calls. With a longer silence detection delay, VAD reacts to the silence of an idle voice channel, but not to pauses in conversation.

This command does not affect voice codecs that have ITU-standardized built-in VAD features—for example, G.729B, G.729AB, G.723.1A. The VAD behavior and parameters of these codecs are defined exclusively by the applicable ITU standard.

Examples

The following example configures a 20-second delay before VAD silence detection is enabled:

```
voice vad-time 20000
```

Related Commands

Command	Description
vad (dial peer)	Enables voice activity detection on a network dial peer.

voice vrf

To configure a voice VRF, use the **voice vrf** command in global configuration mode. To remove the voice VRF configuration, use the **no** form of this command.

voice vrf *vrfname*

no voice vrf *vrfname*

Syntax Description

vrfname	A name assigned to the voice vrf.

Command Default No voice VRF is configured.

Command Modes Global configuration

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines You must create a VRF using the **ip vrf** *vrfname* command before you can configure it as a voice VRF.

To ensure there are no active calls on the voice gateway during a VRF change, voices services must be shut down on the voice gateway before you configure or make changes to a voice VRF.

Examples The following example shows that a VRF called *vrf1* was created and then configured as a voice VRF:

```
ip vrf vrf1
 rd 1:1
 route-target export 1:2
 route-target import 1:2
!
voice vrf vrf1
!
voice service voip
```

Related Commands

Command	Description
ip vrf	Defines a VPN VRF instance and enters VRF configuration mode.

voip-incoming translation-profile

To specify a translation profile for all incoming VoIP calls, use the **voip-incoming translation-profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

voip-incoming translation-profile *name*

no voip-incoming translation-profile *name*

Syntax Description

name	Name of the translation profile.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines Use the **voip-incoming translation-profile** command to globally assign a translation profile for all incoming VoIP calls. The translation profile was previously defined using the **voice translation-profile** command. The **voip-incoming translation-profile** command does not require additional steps to complete its definition.

If an H.323 call comes in and the call is associated with a source IP group that is defined with a translation profile, the source IP group translation profile overrides the global translation profile.

Examples The following example assigns the translation profile named “global-definition” to all incoming VoIP calls:

```
Router(config)# voip-incoming translation-profile global-definition
```

Related Commands

Command	Description
show voice translation-profile	Displays the configurations for all voice translation profiles.
test voice translation-rule	Tests the voice translation rule definition.
voice translation-profile	Initiates a translation profile definition.

voip-incoming translation-rule

To set the incoming translation rule for calls that originate from H.323-compatible clients, use the **voip-incoming translation-rule** command in global configuration mode. To disable the incoming translation rule, use the **no** form of this command.

voip-incoming translation-rule {**calling** | **called**} *name-tag*

no voip-incoming translation-rule {**calling** | **called**} *name-tag*

Syntax Description

name-tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.
calling	Automatic number identification (ANI) number or the number of the calling party.
called	Dial Number Information Service (DNIS) number or the number of the called party.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for VoIP on the Cisco 1750, Cisco AS5300, Cisco 7200, and Cisco 7500 platforms.
12.1(2)T	This command was implemented for VoIP on Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

With this command, all IP-based calls are captured and handled, depending on either the calling number or the called number to the specified tag name.

Examples

The following example identifies the rule set for calls that originate from H.323-compatible clients:

```
Router(config)# voip-incoming translation-rule called 5
```

Related Commands

Command	Description
numbering-type	Matches one number type for a dial-peer call leg.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.

volume

To set the receiver volume level for a POTS port on a router, use the **volume** command in dial peer voice configuration mode. To reset to the default, use the **no** form of this command.

volume *number*

no volume *number*

Syntax Description

number	A number from 1 to 5 representing decibels (dB) of gain. Range is as follows: • 1: –11.99 dB • 2: –9.7dB • 3: –7.7dB • 4: –5.7dB • 5: –3.7dB Default is 3 (–7.7 dB gain).

Command Default 3 (–7.7 dB gain)

Command Modes Dial peer voice configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 803, Cisco 804, and Cisco 813 routers.

Usage Guidelines Set the **volume** command for each POTS port separately. Setting the volume level affects only the port for which it has been set.

Note Only the receiver volume is set with this command.

Use the **show pots volume** command to check the volume status and level.

Examples The following example shows a volume level of 4 for POTS port 1 and a volume level of 2 for POTS port 2.

```
dial-peer voice 1 pots
 destination-pattern 5551111
 port 1
 no call-waiting
 ring 0
 volume 4
```

```
dial-peer voice 2 pots
 destination-pattern 5552222
 port 2
 no call-waiting
 ring 0
 volume 2
```

Related Commands

Command	Description
show pots volume	Shows the receiver volume configured for each POTS port on a router.

vxml allow-star-digit

To configure a Voice Extensible Markup Language (VXML) interpreter to allow the star digit for built-in type digits, use the **vxml allow-star-digit** command in global configuration mode. To disable the configuration, use the **no** form of this command.

vxml allow-star-digit

no vxml allow-star-digit

Syntax Description

This command has no arguments or keywords.

Command Default

A VXML interpreter is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure a VXML interpreter to allow the star digit for built-in type digits:

```
Router# configure terminal
Router(config)# vxml allow-star-digit
```

Related Commands

Command	Description
vxml audioerror	Enables throwing an error event when audio playout fails.
vxml version pre2.0	Enables VoiceXML 2.0 features.

vxml audioerror

To enable throwing an error event when audio playout fails, use the **vxml audioerror** command in global configuration mode. To return to the default, use the **no** form of this command.

vxml audioerror

no vxml audioerror

Syntax Description

This command has no arguments or keywords.

Command Default

An audio error event, error.badfetch, is not thrown when an audio file cannot be played.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Entering this command causes an audio error event, error.badfetch, to be thrown when an audio file cannot be played, for instance, because the file is in an unsupported format, the src attribute references an invalid URI, or the expr attribute evaluates to an invalid URI.

The **vxml audioerror** command overrides the **vxml version 2.0** command, so that if both commands are entered, the audio error event will be thrown when an audio file cannot be played.

Examples

The following example enables the audio error feature:

```
Router(config)# vxml audioerror
```

Related Commands

Command	Description
vxml version pre2.0	Enables features compatible with versions earlier than VoiceXML 2.0.

vxml tree memory

To set the maximum memory size for the VoiceXML parser tree, use the **vxml tree memory** command in global configuration mode. To reset to the default, use the **no** form of this command.

vxml tree memory *size*

no vxml tree memory

Syntax Description

size	Maximum memory size, in kilobytes. Range is 64 to 100000. Default is 1000.

Defaults

1000 KB

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(15)T	The default was changed from 64 to 1000.

Usage Guidelines

This command limits the memory resources available for parsing VoiceXML documents, preventing large documents from consuming excessive system memory. Increasing the maximum memory size for the VoiceXML tree enables calls to use larger VoiceXML documents. If a VoiceXML document exceeds the limit, the gateway aborts the document execution and the **debug vxml error** command displays a "vxml malloc fail" error.

Note In Cisco IOS Release 12.3(4)T and later releases, less memory is consumed when parsing a VoiceXML document because the document is not stored by the VoiceXML tree.

Examples

The following example sets the maximum memory size to 128 KB:

```
vxml tree memory 128
```

Related Commands

Command	Description
debug vxml error	Displays VoiceXML application error messages.
ivr prompt memory	Sets the maximum amount of memory that dynamic audio files (prompts) occupy in memory.
ivr record memory system	Sets the maximum amount of memory for storing all voice recordings on the gateway.

vxml version 2.0

To enable VoiceXML 2.0 features, use the **vxml version 2.0** command in global configuration mode. To return to the default, use the **no** form of this command.

vxml version 2.0

no vxml version 2.0

Syntax Description

This command has no arguments or keywords.

Command Default

The default VoiceXML behavior is compatible with versions earlier than *W3C VoiceXML 2.0 Specification*.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command enables the following VoiceXML features:

- An audio error event, error.badfetch, is not thrown when an audio file cannot be played, for instance, because the file is in an unsupported format, the src attribute references an invalid URI, or the expr attribute evaluates to an invalid URI.
- Support for the beep attribute of the <record> element.
- Blind transfer compliant with *W3C VoiceXML 2.0* and not the same as consultation transfer.
- Compatibility with *W3C VoiceXML 2.0 Specification.*

Examples

The following example enables VoiceXML version 2.0 features:

```
Router(config)# vxml version 2.0
```

Cisco IOS Voice Commands: W

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

watcher all

To allow an external watcher to monitor an internal presentity, use the **watcher all** command in presence configuration mode. To disable monitoring by external watchers, use the **no** form of this command.

watcher all

no watcher all

Syntax Description This command has no arguments or keywords.

Command Default Only internal watchers are allowed when presence is enabled.

Command Modes Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines This command allows external watchers on a remote router connected through a SIP trunk to monitor internal directory numbers. You must enable the **allow watch** command on the internal directory numbers that are watched. To allow external watching from the remote router, you must enable the **allow subscribe** command on the remote router.

Examples The following example shows how to enable external watching of an internal presentity:

```
Router(config)# presence
Router(config-presence)# watcher all
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presentities.
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
presence	Enables presence service on the router and enters presence configuration mode.
presence enable	Allows incoming presence requests from SIP trunks.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.

Command	Description
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

Cisco IOS Voice Commands: Z

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

zone access

To configure the accessibility of your local zone, use the **zone access** command in gatekeeper configuration mode. To remove any accessibility configurations, use the **no** form of this command.

zone access *local-zone-name* {**default | remote-zone** *remote-zone-name*} {**direct | proxied**}

no zone access *local-zone-name* **remote-zone** *remote-zone-name*

Syntax Description

local-zone-name	Name of local zone (synonymous with local gatekeeper).
default	Use with the **direct** or **proxied** keyword to define the mode of behavior for all remote zones that have not been specially named using the **remote-zone** *remote-zone-name* keyword and argument combination.
remote-zone *remote-zone-name*	Name of remote zone (synonymous with remote gatekeeper) for which a special mode of behavior is defined.
direct	Configures direct calls (without use of proxies) between endpoints. The local zone (or gatekeeper) offers the local endpoint IP address instead of the IP address of a local proxy.
proxied	Configures calls using proxies between endpoints. The local zone (or gatekeeper) offers the IP address of a local proxy instead of the local endpoint address.

Command Default

The local zone allows proxied access for all remote zones.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.

Usage Guidelines

By default, a gatekeeper offers a local proxy IP address when queried by a remote gatekeeper about a target local endpoint. This is considered proxied access. By using the **zone access** command, you can configure the local gatekeeper to offer the local endpoint address instead of the local proxy address. This is considered direct access.

Note The **zone access** command, configured on your local gatekeeper, affects only the use of proxies for incoming calls (that is, it does not affect the use of local proxies for outbound calls). When originating a call, a gatekeeper uses a proxy only if the remote gatekeeper offers a proxy at the remote end. A call between two endpoints in the same zone is always a direct (nonproxied) call.

You can define the accessibility behavior of a local zone relative to certain remote zones using the **remote-zone** *remote-zone-name* keyword and argument combination with the **direct** or **proxied** keyword. You can define the default behavior of a local zone relative to all other remote zones using the **default** keyword with the **direct** or **proxied** keywords. To remove an explicitly named remote zone so that it is governed by the default-behavior rule, use the **no zone access** command.

Examples

The following example allows direct access to the local zone eng.xyz.com from remote zones within xyz corporation. All other remote locations will have proxied access to eng.xzy.com.

```
zone local eng.xyz.com xyz.com
zone access eng.xyz.com remote-zone mfg.xyz.com direct
zone access eng.xyz.com remote-zone mktg.xyz.com direct
zone access eng.xyz.com remote-zone sales.xyz.com direct
zone access eng.xyz.com default proxied
```

The following example supposes that only local gatekeepers within xyz.com have direct access to each other because your corporation has firewalls or you do not advertise your gatekeepers externally. You have excellent Quality of Service (QoS) within your corporate network, except for a couple of foreign offices. In this case, use proxies with the foreign offices (in Milan and Tokyo) and nowhere else.

```
zone local sanjose.xyz.com xyz.com
zone access sanjose.xyz.com default direct
zone access sanjose.xyz.com remote-zone milan.xyz.com proxied
zone access sanjose.xyz.com remote-zone tokyo.xyz.com proxied
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

zone bw

To set the maximum bandwidth allowed in a gatekeeper zone at any one time, use the **zone bw** command in gatekeeper configuration mode. To remove the maximum bandwidth setting and make the bandwidth unlimited, use the **no** form of this command.

zone bw *gatekeeper-name max-bandwidth*

no zone bw *gatekeeper-name max-bandwidth*

Syntax Description

gatekeeper-name	Name of the gatekeeper that controls the zone.
max-bandwidth	Maximum bidirectional bandwidth, in kbps, allowed in the zone at any one time.

Command Default

Bandwidth is unlimited.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.

Examples

The following example sets the maximum bandwidth to 1000 kbps for zone gk1:

```
zone bw gk1 1000
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.

zone circuit-id

To associate a remote zone with a circuit, use the **zone circuit-id** command in gatekeeper configuration mode. To delete the circuit ID for a zone, use the **no** form of this command.

zone circuit-id *remote-zone-name circuit-id* [**override-source-circuitid**]

no zone circuit-id *remote-zone-name circuit-id*

Syntax Description

remote-zone-name	Name of the remote zone.
circuit-id	ID of the circuit to be associated with the remote zone.
override-source-circuitid	(Optional) Specifies whether the source circuit ID of the incoming location request (LRQ) message needs to be overridden with this keyword.

Command Default

The override flag is disabled and the incoming source circuit ID is used if present.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(14)T	The **override-source-circuitid** keyword was added.

Usage Guidelines

VoIP calls with an LRQ message that come to a gatekeeper from a non-cisco gatekeeper in a remote zone (for example, from an Internet telephony service provider [ITSP]), the LRQ message does not include a source circuit identifier. This command allows the gatekeeper to assign a circuit identifier to the zone and an IP address of the call origination. If the source circuit ID is already present then the configured value will not be used. To enforce the usage of configured source circuit ID, even if the incoming LRQ has a value, configure the **override-source-circuitid** keyword. The Gatekeeper Transaction Message Protocol (GKTMP) server application uses this data to determine a route for the call.

Examples

The following example configures the remote zone GKout1 with a circuit ID CarrierA:

```
Router(config)# gatekeeper
Router(config-gk)# zone circuit-id GKout1 CarrierA
```

The following example configures the remote zone GKout2 with a circuit ID CarrierB and overrides the incoming LRQ source circuit-id value:

```
Router(config)# gatekeeper
Router(config-gk)# zone circuit-id GKout2 CarrierB override-source-circuitid
```

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
show gatekeeper circuits	Displays circuit information on the gatekeeper.
show gatekeeper endpoint circuits	Displays information for all registered endpoints and carriers for the gatekeeper.

zone cluster local

To define a local grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster local** command in gatekeeper configuration mode. To disable the local grouping of gatekeepers, use the **no** form of this command.

zone cluster local *cluster-name local-zone-name*

no zone cluster local

Syntax Description

cluster-name	Cluster name.
local-zone-name	Local zone name.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines

Use this command to define a local cluster of gatekeepers that are alternates of each other. Each of these gatekeepers must be configured in a compatible manner for the cluster to work effectively.

Examples

The following example defines a local grouping of gatekeepers named EuropeCluster in the ParisGK time zone:

```
zone cluster local EuropeCluster ParisGK
```

Related Commands

Command	Description
element	Defines component elements of local or remote clusters.
zone cluster remote	Defines a remote grouping of gatekeepers, including the gatekeeper that you are configuring.

zone cluster remote

To define a remote grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster remote** command in gatekeeper configuration mode. To disable the remote grouping of gatekeepers, use the **no** form of this command.

zone cluster remote *cluster name* [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]

no zone cluster remote

Syntax Description

cluster name	Cluster name.
cost	(Optional) Cost.
cost-value	(Optional) Cost value. Range is from 1 to 100. The default is L50.
priority	(Optional) Priority.
priority-value	(Optional) Priority value. Range is from 1 to 100. The default is 50.
foreign-domain	(Optional) Cluster is in a different administrative domain.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **foreign-domain** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(13)T3	The **invia** and **outvia** keywords were added.

Usage Guidelines

Use this command to define a set of remote gatekeepers that act as alternates to each other and that form a local cluster. This command causes the gatekeeper to optimize these remote gatekeepers by round-robin sending of Location Request (LRQ) messages.

Examples

The following example shows how to define a remote grouping of gatekeepers:

```
zone cluster remote AsiaCluster cost 70 priority 10
```

Related Commands

Command	Description
element	Defines component elements of local or remote clusters.
zone cluster local	Defines a local grouping of gatekeepers, including the gatekeeper that you are configuring.
zone local	Specifies a zone controlled by a gatekeeper.

zone qos

To configure the Differentiated Services Code Point (DSCP) value for a specific zone or a common DSCP value for all zones in Quality of Service (QoS) configurations on a Cisco router, use the **zone qos** command in gatekeeper configuration mode. To remove the DSCP configuration, use the **no** form of this command.

zone qos {*gatekeeper-name* | **global**} **dscp** *dscp-value*

no zone qos {*gatekeeper-name* | **global**} **dscp** dscp-value

Syntax Description

gatekeeper-name	The gatekeeper name to be configured.
global	Configures the DSCP value globally.
dscp	Specifies the DSCP to be configured.
dscp-value	The predefined DSCP keyword or its equivalent numeric value. Refer to Table 263 for more details.

Command Default

This command is disabled by default.

Command Modes

Gatekeeper configuration (conf-gk)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

To configure a common DSCP value for all local and remote zones, use the **global** keyword and then specify the **dscp** keyword and its value. To change a globally configured DSCP value for a zone-specific DSCP value, the globally configured value should be removed first using the **no** form of the command. If not, a warning message will be displayed. Use the gatekeeper name and the **dscp** keyword with the specific value to configure a zone-based DSCP value.

DSCP can be configured using the predefined DSCP keywords or its equivalent numeric value. For example, to configure the DSCP value of a zone, the **cs1** keyword can be replaced with the numeric value 8. However, the **show gatekeeper zone status** output displays the configured DSCP as cs1. Table 263 provides the predefined DSCP keywords and their equivalent numeric values. The hexadecimal value is the number that is displayed in the QOS field of the IP header.

Table 263 Predefined DSCP Keywords and Numeric Values

Keyword	Numeric Value	Hexadecimal Value
default	0	0x00
cs1	8	0x20
af11	10	0x28
af12	12	0X30

Table 263 Predefined DSCP Keywords and Numeric Values (continued)

Keyword	Numeric Value	Hexadecimal Value
af13	14	0x38
cs2	16	0x40
af21	18	0x48
af22	20	0x50
af23	22	0x58
cs3	24	0x60
af31	26	0x68
af32	28	0x70
af33	30	0x78
cs4	32	0x80
af41	34	0x88
af42	36	0x90
af43	38	0x98
cs5	40	0xA0
ef	46	0xB8
cs6	48	0xC0
cs7	56	0xE0

Examples

The following example shows how to configure the DSCP value for a specific zone using the **zone qos** *gatekeeper-name* **dscp** *dscp-value* command:

```
Router(config)# gatekeeper
Router(conf-gk)# zone qos GK-08 dscp cs3
```

The following example shows how to configure the global DSCP value using the **zone qos global dscp** *dscp-value* command:

```
Router(config)# gatekeeper
Router(conf-gk)# zone qos global dscp af11
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of the zones related to the gatekeeper.

zone local

To specify a zone controlled by a gatekeeper, use the **zone local** command in gatekeeper configuration mode. To remove a zone controlled by a gatekeeper, use the **no** form of this command.

zone local *gatekeeper-name domain-name* [*ras-IP-address*] [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]

no zone local *gatekeeper-name domain-name* [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]

Syntax Description

gatekeeper-name	Gatekeeper name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the *domain-name* is cisco.com, the *gatekeeper-name* might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the *gatekeeper-name* for each zone should be some unique mnemonic string.
domain-name	The domain name served by this gatekeeper.
ras-IP-address	(Optional) IP address of one of the interfaces on the gatekeeper. When the gatekeeper responds to gatekeeper discovery messages, it signals the endpoint or gateway to use this address in future communications. **Note** Setting this address for one local zone makes it the address used for all local zones.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.
enable-intrazone	Forces all intrazone calls to use the via gatekeeper.

Command Default

No local zone is defined.

Note The gatekeeper cannot operate without at least one local zone definition. Without local zones, the gatekeeper goes to an inactive state when the **no shutdown** command is issued.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.2(11)T	This command was implemented on the Cisco MC3810 and Cisco 7200 series.
12.3(4)T	The **invia**, **outvia**, and **enable-intrazone** keywords were added.

Usage Guidelines

Multiple local zones can be defined. The gatekeeper manages all configured local zones. Intrazone and interzone behavior remains the same (zones are controlled by the same or different gatekeepers).

Only one *ras-IP-address* argument can be defined for all local zones. You cannot configure each zone to use a different RAS IP address. If you define this in the first zone definition, you can omit it for all subsequent zones, which automatically pick up this address. If you set it in a subsequent **zone local** command, it changes the RAS address of all previously configured local zones as well. Once defined, you can change it by reissuing any **zone local** command with a different *ras-IP-address* argument.

If the *ras-IP-address* argument is a Hot Standby Router Protocol (HSRP) virtual address, it automatically puts the gatekeeper into HSRP mode. In this mode, the gatekeeper assumes STANDBY or ACTIVE status according to whether the HSRP interface is on STANDBY or ACTIVE status.

You cannot remove a local zone if there are endpoints or gateways registered in it. To remove the local zone, shut down the gatekeeper first, which forces unregistration.

Multiple zones are controlled by multiple logical gatekeepers on the same Cisco IOS platform.

The maximum number of local zones defined in a gatekeeper should not exceed 100.

This command can also be used to change the IP address used by the gatekeeper.

Examples

The following example creates a zone controlled by a gatekeeper in the domain called “cisco.com”:

```
Router(config)# gatekeeper
Router(config-gk)# zone local easterngk.cisco.com cisco.com
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone subnet	Specifies a zone controlled by a gatekeeper.

zone prefix

To add a prefix to the gatekeeper zone list, use the **zone prefix** command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the **no** form of this command with the **gw-priority** option.

zone prefix *gatekeeper-name e164-prefix* [**blast** | **seq**] [**gw-priority** *priority gw-alias* [*gw-alias*, ...]]

no zone prefix *gatekeeper-name e164-prefix* [**blast** | **seq**] [**gw-priority** *priority gw-alias* [*gw-alias*, ...]]

Syntax Description

gatekeeper-name	Name of a local or remote gatekeeper, which must have been defined by using the **zone local** or **zone remote** command.
e164-prefix	E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers. **Note** Although a dot representing each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.
blast	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which they were listed. The default is **seq**.
seq	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. The default is **seq**.
gw-priority *pri-0-to-10 gw-alias*	(Optional) Defines how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix *e164-prefix*. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. Range is from 0 to 10, where 0 prevents the gatekeeper from using the gateway *gw-alias* for that prefix and 10 places the highest priority on gateway *gw-alias*. The default is 5. To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the *pri-0-to-10* value. *gw-alias* name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the **h323-gateway voip h.323-id** command.

Command Default

No knowledge of the gatekeeper zone prefix or the prefix of any other zone is defined.
Gateway priority is 5.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)Q	This command was introduced.
11.3(7)NA	This command was modified for H.323 Version 1.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM	The command was implemented on Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.

If you need a gatekeeper to handle more than one prefix, but for cost reasons you want to be able to group its gateways by prefix usage, there are two ways to do it.

The first method is simpler, has less overhead, and is recommended if your gateways can be divided into distinct groups, in which each group is to be used for a different set of prefixes. For instance, if a group of gateways is used for calling area codes 408 and 650, and another group is used for calling area code 415, you can use this method. In this case, you define a local zone for each set of prefixes and have the group of gateways to be used for that set of prefixes register with that specific local zone. Do not define any gateway priorities. All gateways in each local zone are treated equally in the selection process.

However, if your gateways cannot be cleanly divided into nonintersecting groups (for instance, if one gateway is used for calls to 408 and 415 and another gateway is used for calls to 415 and 650), you can put all these gateways in the same local zone and use the **gw-priority** option to define which gateways will be used for which prefixes.

When choosing a gateway, the gatekeeper first looks for the longest zone prefix match; then it uses the priority and the gateway status to select from the gateways.

If all gateways are available, the gatekeeper chooses the highest-priority gateway. If all the highest-priority gateways are busy (see the gateway **resource threshold** command), a lower-priority gateway is selected.

Note The **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Examples

The following example shows how you can define multiple local zones for separating your gateways:

```
Router(config-gk)# zone local gk408or650 xyz.com
Router(config-gk)# zone local gk415 xyz.com
Router(config-gk)# zone prefix gk408or650 408.......
Router(config-gk)# zone prefix gk408or650 650.......
Router(config-gk)# zone prefix gk415 415.......
```

Now you need to configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415. On Cisco voice gateways, you configure the gateways to register with the appropriate gatekeepers by using the **h323 voip id** command.

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways are used for calling different area codes:

```
Router(config-gk)# zone local localgk xyz.com
Router(config-gk)# zone prefix localgk 408.......
Router(config-gk)# zone prefix localgk 415....... gw-priority 10 gw1 gw2
Router(config-gk)# zone prefix localgk 650....... gw-priority 0 gw1
```

The commands shown accomplish the following tasks:

- Domain xyz.com is assigned to gatekeeper localgk.
- Prefix 408..... is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408..... prefix; selection is made from the master list for the zone.
- Prefix 415..... is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2.
- Prefix 650..... is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1.

A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650. When gateway gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows:

- For gateway pool for 415, gateway gw2 is set to priority 10.
- For gateway pool for 650, gateway gw2 is set to priority 5.

The following example changes gateway gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415....... gw-priority 10 gw2
```

The following example changes both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415....... gw-priority 10 gw1 gw2
```

In this example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. The following example removes the prefix and all associated gateways and priorities from this gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415.......
```

Related Commands

Command	Description
register	Configures a gateway to register or deregister a fully qualified dial-peer E.164 address with a gatekeeper.
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.
zone local	Specifies a zone controlled by a gatekeeper.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

zone remote

To statically specify a remote zone if domain name service (DNS) is unavailable or undesirable, use the **zone remote** command in gatekeeper configuration mode. To remove the remote zone, use the **no** form of this command.

zone remote *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address* [*port-number*] [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]

no zone remote *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address* [*port-number*] [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]

Syntax Description

other-gatekeeper-name	Name of the remote gatekeeper.
other-domain-name	Domain name of the remote gatekeeper.
other-gatekeeper-ip-address	IP address of the remote gatekeeper.
port-number	(Optional) RAS signaling port number for the remote zone. Range is from 1 to 65535. If the value is not set, the default is the well-known RAS port number 1719.
cost *cost-value*	(Optional) Cost of the zone. Range is from 1 to 100. The default is 50.
priority *priority-value*	(Optional) Priority of the zone. Range is from 1 to 100. The default is 50.
foreign-domain	(Optional) Cluster is in a different administrative domain.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.

Command Default

No remote zone is defined. DNS will locate the remote zone.
Default RAS port is 1719.
Cost value is 50.
Priority value is 50.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **cost** and **priority** keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **foreign-domain** keyword was added.

Release	Modification
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850 universal gateways.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and was implemented on the Cisco 7200 series. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T3	The **invia** and **outvia** keywords were added.

Usage Guidelines

Not all gatekeepers have to be in the DNS. For those that are not, use the **zone remote** command so that the local gatekeeper knows how to access them. In addition, you may wish to improve call response time slightly for frequently accessed zones. If the **zone remote** command is configured for a particular zone, you do not need to make a DNS lookup transaction.

The maximum number of zones defined on a gatekeeper varies depending on the mode or the call model or both. For example, a directory gatekeeper may be in the mode of being responsible for forwarding Location Request (LRQ) messages and not handling any local registrations and calls; the call model might be E.164 addressed calls instead of H.323-ID addressed calls.

For a directory gatekeeper that does not handle local registrations and calls, the maximum remote zones defined should not exceed 10,000; an additional 4 MB of memory is required to store this maximum number of remote zones.

For a gatekeeper that handles local registrations and only E.164 addressed calls, the number of remote zones defined should not exceed 2000.

For a gatekeeper that handles H.323-ID calls, the number of remote zones defined should not exceed 200.

When there are several remote zones configured, they can be ranked by cost and priority value. A zone with a lower cost value and a higher priority value is given preference over others.

Examples

The following example configures the local gatekeeper to reach targets of the form *xxx*.cisco.com by sending queries to the gatekeeper named “sj3.cisco.com” at IP address 10.1.1.12.

```
Router(config)# gatekeeper
Router(config-gk)# zone remote sj3.cisco.com cisco.com 10.1.1.12
```

The following example shows how to configure the cost and priority for the gatekeeper “GK10” that serves zone 1.

```
Router(config)# gatekeeper
Router(config-gk)#  zone remote GK10 Zone1 209.165.200.224 cost 20 priority 5
```

Related Commands

Command	Description
show proxy h323 calls	Lists each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

zone subnet

To configure a gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets, use the **zone subnet** command in gatekeeper configuration mode. To disable the gatekeeper from acknowledging discovery and registration messages from subnets or to remove subnets entirely, use the **no** form of this command.

zone subnet *local-gatekeeper-name* {**default** | *subnet-address* {*/bits-in-mask* | *mask-address*}} **enable**

no zone subnet *local-gatekeeper-name* {**default** | *subnet-address* {*/bits-in-mask* | *mask-address*}} **enable**

Syntax Description

local-gatekeeper-name	Name of the local gatekeeper.
default	Applies to all other subnets that are not specifically defined by the **zone subnet** command.
subnet-address	Address of the subnet being defined.
/bits-in-mask	Number of bits of the mask to be applied to the subnet address.
mask-address	Mask (in dotted string format) to be applied to the subnet address.
enable	Gatekeeper accepts discovery and registration from the specified subnets.

Command Default

The local gatekeeper accepts discovery and registration requests from all subnets. If the request specifies a gatekeeper name, it must match the local gatekeeper name or the request is not accepted.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

You can use the **zone subnet** command more than once to create a list of subnets controlled by a gatekeeper. The subnet masks do not have to match actual subnets in use at your site. For example, to specify a particular endpoint, you can supply its address with a 32-bit netmask.

Examples

The following example starts by disabling the gatekeeper, gk1.cisco.com, from accepting discovery and registration messages from all subnets. Next, gk1.cisco.com is configured to accept discovery and registration messages from all H.323 nodes on the subnet 172.21.127.0.

In addition, gk1.cisco.com is configured to accept discovery and registration messages from a particular endpoint with the IP address 172.21.128.56.

```
no zone subnet gk1.cisco.com default enable
zone subnet gk1.cisco.com 172.21.127.0/24 enable
zone subnet gk1.cisco.com 172.21.128.56/32 enable
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
zone local	Specifies a zone controlled by a gatekeeper.