A

aal2-profile custom

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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 code points 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 (config)

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 user agent 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 user agent configuration (config-sip-ua)

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 (cfg-source-grp)

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 ipaccess-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 (config-annexg)

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.

access-secure

To specify that the secure (encrypted) mode is to be used for accessing the session border controller (SBC), use the **access-secure** command in phone proxy configuration mode. To remove the secure mode, use the **no** form of the command.

access-secure
no access-secure

This command has no arguments or keywords.

Command Default

The non-secure mode is used for communication with the SBC.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to specify that the secure (encrypted) mode is to be used for accessing the SBC:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# access-secure
```

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 invoice 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.
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** [**-tacctTempName**] 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

RSVP makes no bandwidth reservations.

Command Modes

Dial-peer configuration (config-dial-peer)

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.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

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 **iprsvpbandwidth** 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.
ip rsvp bandwidth	Enables Resource Reservation Protocol (RSVP) for IP on an interface.

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** 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 (config-tgrep)

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-hiding** command in voice service voip 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 arguments.

Command Default

Signaling and media addresses are visible to all endpoints.

Command Modes

Voice service voip configuration (config-voi-serv)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

All SIP methods or messages must 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.

This command modifies specific supplementary service headers and changes them appropriately from the in-leg to the out-leg.

Those headers include the following:

- Refer-To
- Referred-by
- 3xx response contact header
- History-Info
- Diversion

In these headers, an inside IP would be silently passed from the in-leg to the out-leg by an IP-to-IP gateway resulting in inside IP being sent to the ITSP/Public Internet. When configured with address-hiding the IP-to-IP gateway specifically looks for and changes those headers appropriately to mask the inside IP with its own.

Note Distinctive ringing headers include ringing information and server address where the ringtone can be obtained. These headers are forwarded as is to the peer side even if address hiding is enabled.

Examples

The following example shows 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 are advertised.

Command Default

Static

Command Modes

Annex G configuration (config-annexg)

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	(Optional) Trunk group address family
carrier	(Optional) Carrier code address family
csr	(Optional) Call success rate
ac	(Optional) Available circuits
tc	(Optional) Total circuits

Command Default

No attributes for address families are advertised.

Command Modes

TGREP configuration (config-tgrep)

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 (config-controller)

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 (config-gk)

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

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.

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

Command Modes

Voice-service configuration (config-voi-serv)

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.
12.4(4)T	This command was modified. 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.

Cisco IOS Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

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.
presence enable	Allows incoming presence requests from SIP trunks.

Command	Description
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 (config-dial-peer)

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 SIP configuration mode, or or voice class tenant, or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

anat system
no anat system

Syntax Description

This command has no arguments or keywords.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

Voice service voip-sip configuration (conf-serv-sip)

Dial peer configuration (config-dial-peer)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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
```

The following example shows ANAT being configured per tenant:

```
Router(config-class)# anat system
```

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 (config-voiceport)

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 configuration Router (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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 (config-dial-peer)

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.
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.

Release	Modification
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)ZJ and later releases, the application name default refers to the 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 to 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.

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.

Command	Description
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 (config)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **application** command in dial-peer configuration mode.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models (under voice class tenat configuration) and **package auth**.

Usage Guidelines

Note **custom application** under service is not supported in YANG configuration.

application service APPNAME <app-url> paramspace <options>

Use this command to enter application configuration mode. You can use related commands 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 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.

aqm-register-fnf

To export the audio and video call quality statistics to flow record using Flexible NetFlow collector, use the **aqm-register-fnf** command in global configuration mode. To disable the export of audio and video call quality statistics, use the **no** form of this command.

aqm-register-fnf
no aqm-register-fnf

Syntax Description

This command has no arguments or keywords.

Command Default

The **aqm-register-fnf** command is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **aqm-register-fnf** command when you want to export metrics related to media (voice) quality; for example, conversational mean opinion score (MOS), packet loss rate, conceal ratio, and so on. The **aqm-register-fnf** command must be configured before you use the **media monitoring** command to configure voice quality metrics.

Note Configuring the **no aqm-register-fnf** command does not disable the command in the device's running and startup configurations.

Examples

The following example shows how to enable exporting of audio quality statistics to the flow record:

```
Device> enable
Device# configure terminal
Device(config)# aqm-register-fnf
```

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 (config-gk)

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**arqreject-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 (config-gk)

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 **arqreject-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 **arqreject-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 **zoneprefix** 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 **arqrequest-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 **arqreject-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 (config-iua)

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 xx.x(x)X 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 **showiuaasall**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** *as-name*{*remote-p1* [{[*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**showipsctpassociationparameters** 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 **showipsctpassociationparameters** 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 (config-iua)

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 **showipsctpassociationparameters** 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 enable support for the asserted ID header in incoming Session Initiation Protocol (SIP) requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages, use the **asserted-id** command in voice service VoIP-SIP configuration mode or voice class tenant configuration mode. To disable the support for the asserted ID header, use the **no** form of this command.

asserted-id {**pai** | **ppi**}**system**
no asserted-id system

Syntax Description

pai	(Optional) Enables the P-Asserted-Identity (PAI) privacy header in incoming and outgoing SIP requests or response messages.
ppi	(Optional) Enables the P-Preferred-Identity (PPI) privacy header in incoming SIP requests and outgoing SIP requests or response messages.
system	Specifies that the asserted-id use the global forced CLI setting. This keyword is available only for the tenant configuration mode.

Command Default

The privacy information is sent using the Remote-Party-ID (RPID) header or the FROM header.

Command Modes

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

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)T	This command was introduced.
15.1(3)T	This command was modified. Support for incoming calls was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

If you choose the **pai** keyword or the **ppi** keyword, the gateway builds the PAI header or the PPI header, respectively, into the common SIP stack. The **pai** keyword or the **ppi** keyword has the priority over the Remote-Party-ID (RPID) header, and removes the RPID header from the outbound message, even if the router is configured to use the RPID header at the global level.

Examples

The following example shows how to enable support for the PAI privacy header:

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

The following example shows asserted ID used in the voice class tenant configuration mode:

```
Router(config-class)# asserted-id system
```

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.
voice-class sip asserted-id	Enables support for the asserted ID header in incoming and outgoing SIP requests or response messages in dial-peer configuration mode.

associate application

To associate an application to the digital signal processor (DSP) farm profile, use the **associateapplication**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 (config-dspfarm-profile)

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 Communications Manager with a Cisco Unified Communications Manager 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 Communications Manager from a Cisco Unified Communications Manager 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 Communications Manager. Range is 1 to 50. There is no default value.
priority *priority-number*	Priority of the Cisco Unified Communications Manager within the Cisco Unified Communications Manager 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 (config-sccp-ccm)

Command History

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

Examples

The following example associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 9 and sets the priority of the Cisco Unified Communications Manager within the group to 2:

```
Router(config)# sccp ccm group 9
Router(config-sccp-ccm)# associate ccm 25 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 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 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 **associateprofile**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 (conig-sccp-ccm)

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(config-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 **associateregistered-number** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To remove the association, use the **no** form of this command.

associate registered-number *number* **system**
no associate registered-number

Syntax Description

number	Registered number. The number must be between 4 and 32.
system	Use the global sip-ua associate configuration.

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)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.1(2)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

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
```

The following example shows how to associate a registered number in the voice class tenant configuration mode:

```
Router(config-class)# associate registered-number system
```

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 **asymmetricpayload** command in SIP configuration mode or voice class tenant 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)

Voice class tenant configuration (config-class)

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.
15.6(2) and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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
```

The following example shows how to set up a full asymmetric payload globally in the voice class tenant configuration mode:

```
Router(config-class)# asymmetric payload system
```

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 **atmscramble-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 **atmvideoaesa** 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 **attributeacct-session-idoverloaded** 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 (config-gw-accounting-aaa)

Command History

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

Usage Guidelines

The **attributeacct-session-idoverloaded**command replaces the **gw-accountingh323**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 **attributeh323-remote-idresolved**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 (config-gw-accounting-aaa)

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 **attributeh323-remote-idresolved** command replaces the **gw-accountingh323resolve**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-dial-peer)

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

Related Commands

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

audio forced

To allow only audio and image (for T.38 Fax) media types, and drop all other media types (such as video and application), use the **audio forced** command in voice service voip sip configuration mode. To disable, use **no** form of this command.

audio forced
no audio forced

Command Default

Along with audio and image (for T38 fax) media types, all other media types (such as video and application) are also allowed.

Command Modes

voice service voip sip configuration (conf-serv-sip).
Voice class tenant configuration (config-class).

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Denali 16.3.1	This command was integrated into Cisco IOS XE Denali 16.3.1.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use **audio forced** command to globally allow only audio and image media types.

Example

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

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-promptload**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 **authenticateredirecting-number** command in voice service SIP configuration mode or voice class tenant 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 system
no authenticate redirecting-number

Syntax Description

system	Specifies that the authenticate redirecting-number use the global forced CLI setting. This keyword is available only for the tenant configuration mode.

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)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

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 **authenticateredirecting-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-classsipauthenticateredirecting-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-classsipauthenticateredirecting-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
```

The following example shows how to authenticate a re-directed number in the voice class tenant configuration mode:

```
Router(config-class)# authenticate redirecting-number system
```

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**|**6**|**7**} *password* [**realm** *realm* [**challenge**]]
no authentication {**username** *username* **password** {**0**|**6**|**7**} *password* [**realm** *realm* [**challenge**]] | **all**}

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	Specifies encryption type as cleartext (no encryption).
6	Specifies secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES). **Note** Requires AES primary key to be preconfigured.
7	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.
all	(Optional) Specifies all the authentication entries for the user (dial-peer).

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.
15.2(3)T	This command was modified. The **all** keyword was added to the **no** form of the command.
IOS XE 16.11.1a	Secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES) was introduced.

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.
- Use the **no authentication all** command to remove all the authentication entries for the user.

It is mandatory to specify the encryption type for the password. If a clear text password (type **0**) is configured, it is encrypted as type **6** before saving it to the running configuration.

If you specify the encryption type as **6** or **7**, the entered password is checked against a valid type **6** or **7** password format and saved as type **6** or **7** respectively.

Type-6 passwords are encrypted using AES cipher and a user-defined primary key. These passwords are comparatively more secure. The primary key is never displayed in the configuration. Without the knowledge of the primary key, type **6** passwords are unusable. If the primary key is modified, the password that is saved as type 6 is re-encrypted with the new primary key. If the primary key configuration is removed, the type **6** passwords cannot be decrypted, which may result in the authentication failure for calls and registrations.

Note When backing up a configuration or migrating the configuration to another device, the primary key is not dumped. Hence the primary key must be configured again manually.

To configure an encrypted preshared key, see Configuring an Encrypted Preshared Key.

Note The encryption type **7** is supported in IOS XE Release 16.11.1a, but will be deprecated in the later releases. Following warning message is displayed when encryption type **7** is configured.

```
Warning: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password type 6.
```

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 6 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 6 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 or voice class tenant configuration mode. To disable SIP digest authentication, use the **no** form of this command.

authentication username *username* **password** { **0** | **6** | **7** } *password* [**realm** *realm*]
no authentication { **username** *username* **password** { **0** | **6** | **7** } *password* [**realm** *realm*] | **all** }

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	Specifies encryption type as cleartext (no encryption), which is the default.
6	Specifies secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES). **Note** Requires AES primary key to be preconfigured.
7	Specifies encryption type as encrypted.
password	A string representing the password for authentication. If no encryption type is specified, the password is cleartext format. The string must be between 4 and 128 characters.
realm *realm*	(Optional) A string representing the domain where the credentials are applicable.
all	(Optional) Specifies all the authentication entries for the user (sip-ua).

Command Default

SIP digest authentication is disabled.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.2(3)T	This command was modified. The **all** keyword was added to the **no** form of the command.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
IOS XE 16.11.1a	Secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES) was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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 you provide 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 that is 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.
- Use the **no authentication all** command to remove all the authentication entries for the user.

It is mandatory to specify the encryption type for the password. If a cleartext password (type **0**) is configured, it is encrypted as type **6** before saving it to the running configuration.

If you specify the encryption type as **6** or **7**, the entered password is checked against a valid type **6** or **7** password format and saved as type **6** or **7** respectively.

Type-6 passwords are encrypted using AES cipher and a user-defined primary key. These passwords are comparatively more secure. The primary key is never displayed in the configuration. Without the knowledge of the primary key, type **6** passwords are unusable. If the primary key is modified, the password that is saved as type 6 is re-encrypted with the new primary key. If the primary key configuration is removed, the type **6** passwords cannot be decrypted, which may result in the authentication failure for calls and registrations.

Note In YANG, you cannot configure the same username across two different realms.

Note When backing up a configuration or migrating the configuration to another device, the primary key is not dumped. Hence the primary key must be configured again manually.

To configure an encrypted preshared key, see Configuring an Encrypted Preshared Key.

Note The encryption type **7** is supported in IOS XE Release 16.11.1a, but will be deprecated in the later releases. Following warning message is displayed when encryption type **7** is configured.

```
Warning: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password type 6.
```

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 6 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 6 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 local host 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 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 method

To set an authentication method at login for calls that come into a dial peer, use the **authenticationmethod** 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 **aaaauthenticationloginh323** 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 **authorizationmethod** 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 **aaaauthorizationexech323** 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 (config)

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**noshutdown** 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 (config-voiceport)

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.

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.
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

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.